

COPY

David C. Parisi (SBN 162248)  
 dparisi@parisihavens.com  
 PARISI & HAVENS LLP  
 15233 Valleyheart Drive  
 Sherman Oaks, CA 91403  
 Telephone: (818) 990-1299  
 Fax: (818) 501-7852

Joseph H. Malley (not yet admitted)  
 malleylaw@gmail.com  
 LAW OFFICE OF JOSEPH H. MALLEY, P.C.  
 1045 North Zang Blvd  
 Dallas, TX 75208  
 Telephone: (214) 943-6100  
 Fax: (214) 943-6170

*Counsel for Plaintiffs*

IN THE UNITED STATES DISTRICT COURT  
 FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MATTHEW HINES; JENNIFER AGUIRRE;  
 ALEXANDER HERNANDEZ; individuals, on  
 behalf of themselves and others similarly situated,

Plaintiffs,

v.

OPENFEINT, INC., a Delaware Corporation; and  
 GREE INTERNATIONAL, INC., a California  
 Corporation

Defendants.

FILED  
 2011 JUN 22 P 3:23  
 RICHARD W. WIEKING  
 CLERK, U.S. DISTRICT COURT  
 NORTHERN DISTRICT OF CALIFORNIA

E-filing

EDL  
 CV 11 3084

CASE NO.

JURY DEMAND

**CLASS ACTION COMPLAINT  
 FOR:**

1. Violations of Computer Fraud and Abuse Act, 18 U.S.C. §1030;
2. Violations of the Electronic Communications Privacy Act 18 U.S.C. §2510;
3. Violations of California's Computer Crime Law, Penal Code § 502;
4. Violations of the California Invasion of Privacy Act, Penal Code § 630;
5. Violations of the Consumer Legal Remedies Act, ("CLRA")

BY FAX

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

- California Civil Code § 1750;
- 6. Violation of Unfair Competition, California Business and Professions Code § 17200;
- 7. Breach of Contract;
- 8. Breach of Implied Covenant of Good Faith and Fair Dealing;
- 9. Conversion;
- 10. Negligence; and
- 11. Trespass to Personal Property / Chattels

Plaintiffs, Matthew Hines, Jennifer Aguirre, and Alexander Hernandez, on behalf of themselves and all others similarly situated, by and through their attorneys, Parisi & Havens LLP; and the Law Office of Joseph H. Malley, P.C., as and for their complaint, and demanding trial by jury, allege as follows upon information and belief, based upon, *inter alia*, investigation conducted by and through their attorneys, which are alleged upon knowledge, sue Defendants OpenFeint, Inc., and GREE International, Inc. Plaintiffs’ allegations as to themselves and their own actions, as set forth herein are based upon their personal knowledge, and all other allegations are based upon information and belief pursuant to the investigations of counsel. Based upon such investigation, Plaintiffs believe that substantial evidentiary support exists for the allegations herein or that such allegations are likely to have evidentiary support after a reasonable opportunity for further investigation and discovery.

**NATURE OF THE ACTION**

1. Plaintiffs bring this consumer Class Action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3) on behalf of themselves and a class of similarly situated Internet users (each a “Class Member” of the putative “Class”) who were victims of privacy violations, and unfair and deceptive business wherein their privacy and security rights

1 were violated by Defendant OpenFeint, Inc., (hereinafter referred to as “OpenFeint” or  
 2 “Defendant”) and Defendant GREE International, Inc. (hereinafter referred to as “GREE”);  
 3 hereinafter collectively referred to as “Defendant OpenFeint.” Defendant OpenFeint  
 4 individually, and in concert, with third parties gained unauthorized access to, and unauthorized  
 5 use of, Plaintiffs’ and Class Members’ mobile devices used for communication over a cellular  
 6 network which include internet and multimedia capabilities (hereinafter collectively referred to  
 7 as “mobile devices”) in order to access, collect, monitor, and remotely store, without notice or  
 8 consent, Plaintiffs’ and Class Members’ mobile device’s Unique Device Identifiers (hereinafter  
 9 referred to as “UDIDs”), Personally Identifiable Information, OpenFeint user account, GPS  
 10 “Fine” co-ordinates (user’s exact latitude and longitude), and Facebook/Twitter profiles, linking  
 11 the aggregated data with the Plaintiffs’ and Class Members’ UDIDs for financial gain.  
 12

13         2.         The nature of this Class Action includes a sequence of events and consequences  
 14 wherein entities that develop mobile applications (hereinafter collectively referred to as  
 15 “Application Developers”), Advertising Networks, and Web Analytic Vendors associated to  
 16 market mobile applications; (hereinafter collectively referred to as “Application Developer’s  
 17 Affiliates”), gained individually and in concert with Defendant OpenFeint, unauthorized access  
 18 to, transmittal of, and use of data, which included but was not limited to, the Plaintiffs’ and Class  
 19 Members’ UDIDs, obtained from the Plaintiffs’ and Class Members’ mobile devices. Data was  
 20 acquired by bypassing both the technical and code based barriers intended to limit such access,  
 21 and the Plaintiffs’ and Class Members’ privacy and security settings. Defendant perpetuated this  
 22 fraudulent activity and deceptive practice, knowingly, and with the intent to transmit and access  
 23 Personally Identifiable Information obtained, in whole or part, by its use of the Plaintiffs’ and  
 24 Class Members’ mobile devices for unauthorized purposes.  
 25

26         3.         Defendant OpenFeint acted independently, and in concert with Application  
 27  
 28

1 Developers and Application Developer's Affiliates, knowingly authorizing, directing, ratifying,  
 2 approving, acquiescing in, or participating in conduct, made the basis of this Class Action, which  
 3 included, but was not limited to, the unauthorized access to and unauthorized use of the  
 4 Plaintiffs' and Class Members' mobile devices UDIDs.

5 4. Defendant OpenFeint's business plan involved unauthorized access to, and  
 6 disclosure of, Personal Information ("PI"), Personally Identifiable Information ("PII"), Sensitive  
 7 Identifying Information ("SII"), and the user's exact latitude and longitude, GPS "Fine" co-  
 8 ordinates ("Fine GPS"), obtained from the Plaintiffs' and Class Members' mobile devices, using  
 9 their UDIDs to aggregate Plaintiffs' and Class Members' data, which the Defendant  
 10 accomplished covertly, without adequate notice or consent of its users, involving one hundred  
 11 million (100,000,000) consumer mobile devices, circumventing Plaintiffs' and Class Members'  
 12 privacy and security controls, for purposes not disclosed within its Terms of Service and/or  
 13 Privacy Policy, nor the Application Developers, failing to protect Plaintiffs and Class Members,  
 14 involving their privacy and endangering their physical security, causing harm and economic  
 15 injury, and accomplished by Defendant OpenFeint for commercial gain. To accentuate the level  
 16 of privacy and security concerns, many of the downloaded applications affiliated with Defendant  
 17 OpenFeint involved the unauthorized tracking of *minor children*.

#### 18 **INTRADISTRICT ASSIGNMENT**

19 5. Defendant OpenFeint, Inc.'s principal executive offices and headquarters are  
 20 located in this District at 330 Primrose Road, Burlingame, California. Intra-district assignment  
 21 to the San Francisco Division is proper.

#### 22 **JURISDICTION AND VENUE**

23 6. Venue is proper in this District under 28 U.S.C. §1391(b) and (c) against  
 24 Defendant. A substantial portion of the events and conduct giving rise to the violations of law  
 25

1 complained of herein occurred in this District and Defendant conduct business with consumers in  
2 this District. Defendant OpenFeint, Inc.'s principle executive offices and headquarters during the  
3 class period were located in this District. Defendant GREE International, Inc.'s principle  
4 executive offices and headquarters during the class period were located in this District.

5 7. This court has Federal question jurisdiction as the complaint alleges violation of  
6 the following: (1) Computer Fraud and Abuse Act, 18 U.S.C. §1030; and (2) Electronic  
7 Communications Privacy Act 18 U.S.C. §2510.

8 8. Subject-matter jurisdiction exists in this Court related to this action pursuant to  
9 the Class Action Fairness Act, 28 U.S.C. § 1332(c). The aggregate claims of Plaintiffs and the  
10 proposed Class Members exceed the sum or value of \$5,000,000.00 exclusive of interests and  
11 costs.  
12

13 9. Venue is proper in this district and vests jurisdiction in the California state and  
14 federal courts in the district of the location of their principal corporate place of businesses. Thus,  
15 mandatory jurisdiction in this U.S. District Court vests for any Class Member, wherever they  
16 reside, for the mobile device activity made the basis of this action which occurred within the  
17 United States. The application of the law of the State of California should be applied to any  
18 mobile device activity made the basis of this action anywhere, within the United States, as if any  
19 and all activity occurred entirely in California and to California resident. Thus, citizens and  
20 residents of all states are, for all purposes related to this instant Complaint, similarly situated  
21 with respect to their rights and claims as California residents, and therefore are appropriately  
22 included as members of the Class, regardless of their residency, or wherever the mobile device  
23 activity occurred made the basis of this action.  
24

25 10. This Court has personal jurisdiction over Defendants OpenFeint and GREE which  
26 maintained their corporate headquarters in, and the acts alleged herein, were committed in  
27  
28

California, within this district, during the class period.

11. Minimal diversity of citizenship exists in this action, providing jurisdiction as proper in the Court, since Defendant is a corporation headquartered in this District during the class period, and Plaintiffs include citizens and residents of this District, and assert claims on behalf of a proposed Class whose members are scattered throughout the fifty states and the U.S. territories; thus there is minimal diversity of citizenship between proposed Class Members and the Defendant.

12. This is the judicial district wherein the basis of the conduct complained of herein involving the Defendant was devised, developed, implemented. The actual interaction of information and data was activated from, and transmitted to and from this District; therefore all evidence of conduct as alleged in this complaint is located in this judicial district.

### **PARTIES**

13. Plaintiff Matthew Hines (“Hines”) is a citizen and resident of Fort Worth, Texas, (Tarrant County, Texas).

14. Plaintiff Jennifer Aguirre (“Aguirre”) is a citizen and resident of Milwaukee, Wisconsin, (Milwaukee County, Wisconsin).

15. Plaintiff Alexander Hernandez (“Hernandez”) is a citizen and resident of Dallas, Texas, (Dallas County, Texas).

16. Defendant OpenFeint, Inc., (“OpenFeint” or “Defendant”) is a Delaware corporation headquartered in California, during the class period, a privately owned corporation, which maintained its headquarters at 330 Primrose Road, Burlingame, Suite 515, California, (San Mateo County, California). Defendant OpenFeint, does business throughout the United States, and in particular, does business in State of California and in this judicial district.

17. Defendant GREE International, Inc., (“GREE” or “Defendant”) is a California

1 corporation headquartered in California, during the class period, a privately owned corporation,  
2 which maintained its headquarters at 1084 De Haro Street, San Francisco, California, (San  
3 Francisco County, California). Defendant GREE, does business throughout the United States,  
4 and in particular, does business in State of California and in this judicial district.

5 **A. Plaintiff Matthew Hines' Experience**

6 18. On information and belief, Plaintiff Matthew Hines incorporates all allegations  
7 within this complaint, and his experiences are the same to all Plaintiffs and Class Members.

8 19. At all relevant times herein, Hines owned a mobile device, operated by a mobile  
9 device operating system, used that mobile device, and on one or more occasions during the class  
10 period, in the city of residence, accessed one (1) or more of the applications, that on information  
11 and belief, are affiliated with the Defendant OpenFeint, which resulted in Defendant OpenFeint  
12 gaining unauthorized access to, and unauthorized use of, Hines' mobile device's UDID.  
13

14 20. As Hines accessed his applications, Defendant OpenFeint, without adequate  
15 notice, or consent, accessed, collected, monitored, and remotely stored, his mobile device's  
16 Unique Device Identifiers.  
17

18 21. In April 2011, Hines became aware of information related to the tracking  
19 activities of one (1) or more of Defendant OpenFeint and its affiliated applications. It is Hines'  
20 belief that Defendant OpenFeint's accessing of his mobile device's UDID permitted tracking  
21 within his mobile device, used for tracking by Defendant OpenFeint, Application Developers,  
22 and Application Developer's Affiliates. Hines did not receive adequate notice of the use of such a  
23 tracking identifier, did not consent to the use of such a tracking identifier, and did not want such  
24 a tracking identifier installed on his mobile device to track his mobile activities.  
25

26 22. Plaintiff Hines considers the information which uniquely identifies his mobile  
27 device to be in the nature of confidential. Plaintiff Hines believes that Personally Identifiable  
28



1 Information should not be obtained or disclosed without adequate notice or consent, and  
2 aggregating his Personally Identifiable Information to link such to his mobile device's UDIDs  
3 violates his privacy and security which resulted in harm.

4 23. Plaintiff Hines believes that if he were to activate the Defendant OpenFeint's  
5 Affiliated Applications, or access the Defendant OpenFeint's App Markets and download  
6 Defendant OpenFeint affiliated applications, the tracking device used by Defendant OpenFeint to  
7 access, collect, monitor, and remotely use the applications to obtain his mobile device's UDIDs  
8 would be used again by the Defendant OpenFeint.  
9

10 **B. Plaintiff Jennifer Aguirre's Experience**

11 24. On information and belief, Plaintiff Jennifer Aguirre incorporates all allegations  
12 within this complaint, and her experiences are the same to all Plaintiffs and Class Members.

13 25. At all relevant times herein, Aguirre owned a mobile device, operated by a mobile  
14 device operating system, used that mobile device, and on one or more occasions during the class  
15 period, in the city of residence, accessed one (1) or more of the applications, that on information  
16 and belief, are affiliated with the Defendant OpenFeint, which resulted in Defendant OpenFeint  
17 gaining unauthorized access to, and unauthorized use of, Aguirre's mobile device's UDID.  
18

19 26. As Aguirre accessed her applications, Defendant OpenFeint, without adequate  
20 notice, or consent, accessed, collected, monitored, and remotely stored, her mobile device's  
21 Unique Device Identifiers.

22 27. In April 2011, Aguirre became aware of information related to the tracking  
23 activities of one (1) or more of Defendant OpenFeint and its affiliated applications. It is Aguirre's  
24 belief that Defendant OpenFeint's accessing of her mobile device's UDID permitted tracking  
25 within her mobile device, used for tracking by Defendant OpenFeint, Application Developers,  
26 and Application Developer's Affiliates. Aguirre did not receive adequate notice of the use of such  
27  
28



1 a tracking identifier, did not consent to the use of such a tracking identifier, and did not want  
2 such a tracking identifier installed on her mobile device to track her mobile activities.

3 28. Plaintiff Aguirre considers the information which uniquely identifies her mobile  
4 device to be in the nature of confidential. Plaintiff Aguirre believes that Personally Identifiable  
5 Information should not be obtained or disclosed without adequate notice or consent, and  
6 aggregating her Personally Identifiable Information to link such to her mobile device's UDIDs  
7 violates her privacy and security which resulted in harm.

8  
9 29. Plaintiff Aguirre believes that if she were to activate the Defendant OpenFeint's  
10 Affiliated Applications, or access the Defendant OpenFeint's App Markets and download  
11 Defendant OpenFeint affiliated applications, the tracking device used by Defendant OpenFeint to  
12 access, collect, monitor, and remotely use the applications to obtain her mobile device's UDIDs  
13 would be used again by the Defendant OpenFeint.

14 **C. Plaintiff Alexander Hernandez's Experience**

15  
16 30. On information and belief, Plaintiff Alexander Hernandez incorporates all  
17 allegations within this complaint, and his experiences are the same to all Plaintiffs and Class  
18 Members.

19 31. At all relevant times herein, Hernandez owned a mobile device, operated by a  
20 mobile device operating system, used that mobile device, and on one or more occasions during  
21 the class period, in the city of residence, accessed one (1) or more of the applications, that on  
22 information and belief, are affiliated with the Defendant OpenFeint, which resulted in Defendant  
23 OpenFeint gaining unauthorized access to, and unauthorized use of, Hernandez's mobile  
24 device's UDID.

25  
26 32. As Hernandez accessed his applications, Defendant OpenFeint, without adequate  
27 notice, or consent, accessed, collected, monitored, and remotely stored, his mobile device's  
28

1 Unique Device Identifiers.

2 33. In April 2011, Hernandez became aware of information related to the tracking  
3 activities of one (1) or more of Defendant OpenFeint and its affiliated applications. It is  
4 Hernandez's belief that Defendant OpenFeint's accessing of his mobile device's UDID permitted  
5 tracking within his mobile device, used for tracking by Defendant OpenFeint, Application  
6 Developers, and Application Developer's Affiliates. Hernandez did not receive adequate notice  
7 of the use of such a tracking identifier, did not consent to the use of such a tracking identifier,  
8 and did not want such a tracking identifier installed on his mobile device to track his mobile  
9 activities.  
10

11 34. Plaintiff Hernandez considers the information which uniquely identifies his  
12 mobile device to be in the nature of confidential. Plaintiff Hernandez believes that Personally  
13 Identifiable Information should not be obtained or disclosed without adequate notice or consent,  
14 and aggregating his Personally Identifiable Information to link such to his mobile device's  
15 UDIDs violates his privacy and security which resulted in harm.  
16

17 35. Plaintiff Hernandez believes that if he were to activate the Defendant OpenFeint's  
18 Affiliated Applications, or access the Defendant OpenFeint's App Markets and download  
19 Defendant OpenFeint affiliated applications, the tracking device used by Defendant OpenFeint to  
20 access, collect, monitor, and remotely use the applications to obtain his mobile device's UDIDs  
21 would be used again by the Defendant OpenFeint.  
22

23 **D. Sequence of Events and Consequences- Plaintiffs and Class Members**

24 36. The sequence of events, and consequences common to Plaintiffs and Class  
25 Members, made the basis of this action, include, but are not limited to the following:

- 26 a) Plaintiffs and Class Members are individuals in the United States who own  
27 and use mobile devices, which include a mobile device operating system,  
28 which provides an application "store" or "market" to download applications. Plaintiffs and Class Members entered into a Licensing Agreement with the

Mobile Device Operating System Manufacturers that operated the application store or market;

- b) Plaintiffs and Class Members then accessed an application affiliated with Defendant OpenFeint, entering into a licensing agreement with one (1) or more of the Application Developers, and installed one (1) or more applications within the class period;
- c) The Application Developers, which developed the applications that the Plaintiffs and Class Members downloaded, had entered into a legally binding agreement with Defendant OpenFeint;
- d) The Application Developers, which developed the applications that the Plaintiffs and Class Members downloaded, had entered into a legally binding agreement with Mobile Device Operating Manufacturers that operated an application “store” or “market”;
- e) The Application Developers were affiliated with one (1) or more Ad networks and Web Analytic Vendors and entered into Licensing Agreements;
- f) Defendant OpenFeint then obtained, without notice or authorization, the Plaintiffs’ and Class Members’ UDIDs, transmitted or allowed access to the UDIDs by its Application Developers which in turn transmitted such to Application Developer Affiliates;
- g) Defendant OpenFeint then took unprecedented liberties, without notice or authorizations, and obtained at will Plaintiffs’ and Class Members’ mobile device’s data, using the mobile device’s UDIDs to aggregate the mobile device data;
- h) Defendant OpenFeint then created, individually and in concert with Application Developers, a database related to Plaintiffs’ and Class Members’ mobile device data, to assist Defendant’s tracking scheme. Such tracking could not be detected, managed or deleted, and provided, in whole or part, the collective mechanism to track Plaintiffs and Class Members, without notice or consent;
- i) Defendant OpenFeint then conducted systematic and continuous surveillance of the Plaintiffs’ and Class Members’ mobile devices activity, which continues to date;
- j) Defendant OpenFeint then copied, used, and stored the mobile device UDIDs, data derived from the Plaintiffs’ and Class Members’ mobile devices, after it knowingly accessed, without authorization, the Plaintiffs’ and Class Members’ mobile device;
- k) Defendant OpenFeint then obtained Plaintiffs’ and Class Members’ Personally Identifiable Information, derived in whole or part, from its monitoring the mobile application activities of Plaintiffs and Class Members. Defendant compiled and misappropriated personal information that includes details about

1 Plaintiffs' and Class Members' profiles to identify individual users to track on  
 2 an ongoing basis, across numerous applications, and tracking when they  
 3 accessed applications from different mobile devices, at home and at work.  
 4 This Sensitive Information may include such things as users' video  
 5 application viewing choices or activities to obtain personal characteristics  
 6 such as: gender, age, race, number of children, education level, geographic  
 7 location, and household income, what was viewed, what was bought,  
 8 materials read, financial situation details, sexual preference, and even more  
 9 specific information like health conditions;

- 10 l) Defendant OpenFeint then linked UDIDs to Defendant OpenFeint user  
 11 accounts, linked UDIDs to GPS "Fine" co-ordinates and to Facebook and/ or  
 12 Twitter profiles;
- 13 m) Defendant OpenFeint then used analytics software to collect, use and disclose  
 14 device data to third parties, an act that violates Plaintiffs' and Class Members'  
 15 mobile device's agreement;
- 16 n) Defendant OpenFeint then provided assurances to Plaintiffs and Class  
 17 Members that any and all authorized applications was safe for downloading;
- 18 o) Defendant OpenFeint then failed to notify and warn Plaintiffs and Class  
 19 Members of its covert activities within their mobile devices, and the covert  
 20 tracking activities by Application Developers and Application Developer's  
 21 Affiliates before, during, and after notice, of the unauthorized practices, made  
 22 the basis of this action, so that Plaintiffs and Class Members could take  
 23 appropriate actions to opt-out of the unauthorized surveillance and/or to delete  
 24 any and all applications;
- 25 p) Defendant OpenFeint then failed to block access to, and void the licensing  
 26 agreements of Application Developers after it received notice of individual  
 27 and concerted actions, made the basis of this action;
- 28 q) Defendant OpenFeint then failed to provide any terms of service, or privacy  
 policy, related to its use of UDIDs for tracking, or provide an updated privacy  
 policy alerting its users of its activities, or the Application Developers and  
 Defendant Application's activity, made the basis of these actions; thus  
 Plaintiffs and Class Members had no notice of such activities, nor the ability  
 to mitigate their harm and damage after the fact;
- r) Defendant OpenFeint then failed to obligate Application Developers to any  
 terms of service, or privacy policy, related to its use of UDIDs for tracking, or  
 provide an updated privacy policy alerting its users of Application Developers  
 and Defendant Application activity, made the basis of these actions; thus  
 Plaintiffs and Class Members had no notice of such activities, nor the ability  
 to mitigate their harm and damage after the fact;
- s) Defendant OpenFeint then failed to obligate Developer's Affiliates notice to  
 Plaintiffs and Class Members of its tracking activities in order to obtain

1 authorization; thus Plaintiffs and Class Members had no notice of such  
2 activities, nor the ability to mitigate their harm and damage after the fact;

- 3 t) Defendant OpenFeint then failed to provide Plaintiffs and Class Members  
4 information within its privacy policies concerning the affiliation of each  
5 Application Developer, its Application Developer's Affiliates, and  
6 information related to the extent of its tracking, made the basis of this action,  
7 nor adequate opt-out information;
- 8 u) Plaintiffs and Class Members that desired to cease tracking by Defendant  
9 OpenFeint by deleting the application, had Defendant continue to track their  
10 activities;
- 11 v) Plaintiffs and Class Members that became aware of Defendant OpenFeint's  
12 association with third parties were unable to restrict access to their UDIDs  
13 from within their own mobile device to cease all tracking;
- 14 w) Plaintiffs and Class Members that became aware that Defendant OpenFeint  
15 had created a database, and deleted the databases to cease any and all tracking,  
16 had the Defendant OpenFeint maintain storage and use of all data derived  
17 from its unauthorized activity;
- 18 x) Defendant OpenFeint then converted the Plaintiffs' and Class Members'  
19 electronic data including, but not limited to, UDIDs for commercial gain;
- 20 y) Plaintiffs and Class Members involved with the Defendant were harmed by its  
21 practices including, but not limited to, the following:
- 22 1. Violations of legally protected Federal, State and Common Law rights  
23 of privacy;
  - 24 2. Financial harm caused to Plaintiffs and Class Members by Defendant's  
25 unauthorized access to "property not provided by users," resulting in  
26 time and expenses incurred to remedy the effects of damages caused to  
27 Plaintiffs' and Class Members' mobile devices;
  - 28 3. Financial harm caused to Plaintiffs and Class Members by Defendant's  
unauthorized collection, use, and sale of "property not provided by  
users," and seized by the Defendant's "data mining" and tracking  
activities that linked Plaintiffs and Class Members' data to the mobile  
device's UDIDs. Plaintiffs and Class Members purchase a mobile  
device from a mobile device manufacturer and cannot resell their  
mobile devices, thus incurring a diminution in "value" of their  
property;
  4. Financial harm caused to Plaintiffs and Class Members by Defendant's  
unauthorized collection, use, and sale of "bandwidth not provided by  
users," and seized from the user's mobile device. Plaintiffs and Class  
Members purchase bandwidth from their provider in order to use their  
mobile devices, and any and all "data mining" conducted by

Defendant required the use of Plaintiffs' and Class Members' bandwidth, thus interrupting and depleting the services purchased, causing the loss of "value" to the bandwidth purchased by Plaintiffs and Class Members;

5. Financial harm caused to Plaintiffs and Class Members by Defendant's unauthorized collection, use, and sale of "property not provided by users," and seized by the Defendant. Plaintiffs and Class Members paid for a mobile device capable of particular levels of processing and internet connectivity services capable of particular transmission speeds. Defendant's activities usurped the Plaintiffs' and Class Members' mobile devices' processing and connectivity resources, thus diminishing its performance;
6. Financial harm caused to Plaintiffs and Class Members by Defendant's unauthorized collection, use, and sale of Plaintiffs' and Class Members' mobile device's UDIDs, "information not provided by users," and seized by Defendant. Such user information constitutes assets with discernable "value," seized and sold by Defendant, thus causing Plaintiffs and Class Members to lose the "value" of their Personal Information;
7. Financial harm caused to Plaintiffs and Class Members by Defendant's unauthorized collection, use, and sale of Plaintiffs' and Class Members' mobile data, "information not provided by users," and seized by Defendant. Such user information constitutes assets with discernable "value," seized and sold by Defendant, thus causing Plaintiffs and Class Members to lose the "value" of their Personal Information;
8. Financial harm caused to Plaintiffs and Class Members by Defendant's unauthorized collection, use, and sale of "information not provided," and seized by Defendant. Plaintiffs and Class Members purchased the products and services associated with the Operating Service within their mobile devices, "paying" for the mobile device and operating system. Defendant provided their Personal Information, a valuable property that was exchanged not only for Defendant's Platform, but also in exchange for Defendant's promise to employ commercially reasonable methods to maintain the Personal Information that was exchanged. Defendant caused a breach of its agreement with Plaintiffs and Class Members' by allowing other parties to obtain such data, thus causing Plaintiffs to lose the "value" of their Personal Information; and
9. Financial harm caused to Plaintiffs and Class Members by Defendant's unauthorized collection, use, and sale of mobile data provided by Plaintiffs and Class Members. The profitability of Defendant's Platform, like most "free" apps, is not ad driven but user data centric. Plaintiffs and Class Members offered limited use of their information as "consideration" to Defendant in return for the use of Defendant's

Platform. Defendant's exploitation of Plaintiffs' and Class Members' mobile devices to obtain and sell their personal information benefitted Defendant with increased profits as opposed to the benefits obtained by Plaintiffs and Class Members who surrendered much more data than they bargained for when they enabled Defendant OpenFeint's Platform.

z) Plaintiffs' and Class Members' allegations, made the basis of this action, as it relates generally to UDIDs, is supported in whole or part by the following recent studies:

- Ashkan Soltani and David Campbell, Electric Alchemy.net, "The Journal's Cellphone Testing Methodology," (last accessed April 15, 2011), online: <http://online.wsj.com/article/SB10001424052748704034804576025951767626460.html>;
- Eric Smith, "iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)" (last accessed April 15, 2011), online: <http://www.pskl.us/wp/wp-content/uploads/2010/09/Android-Applications-Privacy-Issues.pdf>;
- William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, Anmol N. Sheth, "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones" (last accessed April 15, 2011), online: <http://www.appanalysis.org/tdroid10.pdf>; and
- Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna, "PiOS: Detecting Privacy Leaks in iOS Applications," (last accessed April 15, 2011), online: <http://www.technologyreview.com/computing/27128/?pl=A2&a=f>

aa) Plaintiffs' and Class Members' allegations, made the basis of this action as it relates specifically to Defendant OpenFeint's tracking, is supported in whole or part by the following recent studies:

- Aldo Cortesi, "De-anonymizing Apple UDIDs with OpenFeint" (last accessed May 5, 2011), online: <http://corte.si/posts/security/openfeint-udid-deanonymization/index.html>
- Aldo Cortesi, "How UDIDs are used: a survey" (last accessed May 20, 2011), online: <http://corte.si/posts/security/apple-udid-survey/index.html>

37. Defendant's conduct, individually and jointly, is a fraud that has been perpetrated for years, facilitated, and coordinated, by some of the world's largest Application Developers, network advertising industry, and web analytic vendors, thereby costing the Class upwards of hundreds of millions of dollars. Defendant has been systematically defrauding Class Members in a covert operation of surveillance made possible by their gross misconduct, negligence, apparent



coordination, actual fraud, and violation of one (1) or more of the following:

- 1) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the “CFAA”);
- 2) Electronic Communications Privacy Act 18 U.S.C. §2510 (the “ECPA”);
- 3) California’s Computer Crime Law, Penal Code § 502;
- 4) California Invasion of Privacy Act, Penal Code § 630;
- 5) Consumer Legal Remedies Act, (“CLRA”) California Civil Code § 1750;
- 6) Unfair Competition, California Business and Professions Code § 17200;
- 7) Breach of Contract;
- 8) Breach of Implied Covenant of Good Faith and Fair Dealing;
- 9) Conversion;
- 10) Negligence;
- 11) Trespass to Personal Property / Chattels; and

38. Defendant manipulated the Plaintiffs’ and Class Members’ mobile devices, which have computing functions used in and affecting interstate commerce and communication and were therefore protected computers, a conduct in violation as defined in the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030(e)(2).

39. Defendant obtained electronic communications sent to the Plaintiffs’ and Class Members’ mobile device, including but not limited to, the Plaintiffs’ and Class Members’ UDID, information sought to identify the Plaintiffs and Class Members, since such persisted across Internet sessions. Such provided in whole, or part, the ability to identify the users’ mobile device’s functions, a conduct in violation of the Electronic Communications Privacy Act 18 U.S.C. §2510.

40. Defendant’s conduct, made the basis of this action, included but was not limited to, tampering, interference, unauthorized access to Plaintiffs’ and Class Members’ mobile device, a conduct in violation of the California’s Computer Crime Law, California Penal Code § 502.

1           41. Defendant's conduct, made the basis of this action, involved the unauthorized  
2 access to Plaintiffs' and Class Members' electronic communications with one (1) or more entities  
3 based in California, a conduct in violation of the California Invasion of Privacy Act Penal Code §  
4 630 et seq.

5           42. Defendant's conduct, made the basis of this action, was an engagement in unfair  
6 and deceptive acts and practices in the course of transactions with Plaintiffs and Class Members,  
7 and such transactions were intended to and did result in the sale of services, a conduct in  
8 violation of the Consumer Legal Remedies Act, California Civil Code § 1750, et seq.

9           43. Defendant's conduct, made the basis of this action, resulted in acts of deception,  
10 fraud, inconsiderable and unfair commercial practices, concealing, suppressing, and/or omitting  
11 material facts with the intent to have Plaintiffs and Class Members rely upon such concealment,  
12 oppression or omission. Defendant's unfair and deceptive trade acts caused damage and harm to  
13 Plaintiffs and Class Members, a conduct in violation of the Unfair Competition Law, California  
14 Business and Professions Code § 17200.

15           44. Defendant OpenFeint's conduct, made the basis of this action, was a breach of  
16 contract between Defendant OpenFeint and Plaintiffs and Class Members, including but not  
17 limited to, failure to abide by the licensing agreement which forbade release of Personal  
18 Information to third parties without notice and consent. Application Developers' contractual  
19 duties and obligation to Defendant OpenFeint do not release Defendant OpenFeint from its  
20 liability to Plaintiffs and Class Members.

21           45. Application Developers' conduct, made the basis of this action, was a breach of  
22 contract between Application Developers and Plaintiffs and Class Members, including but not  
23 limited to, failure to abide by the licensing agreement which forbade release of Personal  
24 Information to third parties without notice and express consent. Defendant OpenFeint and  
25  
26  
27  
28

1 Application Developer Affiliates' contractual duties and obligation to Application Developers do  
2 not release Application Developers from its liability to Plaintiffs and Class Members.

3 46. Defendant's conduct, made the basis of this action, constitutes a Breach of  
4 Implied Covenant of Good Faith and Fair Dealing including, but not limited to, failure to abide  
5 by its agreement implied that it would not act in bad faith and share information stored on  
6 Plaintiffs' and Class Members' mobile devices.

7 47. Defendant's conduct, made the basis of this action, included acts of conversion  
8 whereby the Plaintiffs' and Class Members' mobile device data, which included Sensitive and  
9 Personally Identifiable Information, was obtained by Defendant, exercising dominion over such  
10 property, and providing to third parties for commercial gain, including an economic loss to  
11 Plaintiffs and Class Members by the Defendant's sale of Plaintiffs' and Class Members' user  
12 data.

13 48. Defendant OpenFeint's conduct, made the bases of this action, was an act of  
14 negligence, including but not limited to, its failure to fulfill its contractual commitments to  
15 Plaintiffs and Class Members' Personally Identifiable Information, privacy, and security, agreed  
16 upon within the terms of Defendant OpenFeint's Terms of use and Privacy Policy for use of the  
17 App Markets.

18 49. Defendant's conduct, made the basis of this action, involved the unauthorized  
19 access to Plaintiffs and Class Members Electronic Communications with one (1) or more entities  
20 based in California, a conduct violation of the Unfair or Deceptive Acts in Violation of Each  
21 State's "Little FTC" Acts.

22 50. Plaintiffs and Class Members own the right to possess the personal property,  
23 including but not limited to, Plaintiffs' and Class Members' data, obtained by the Defendant who  
24 intentionally exercised dominion and control over such user data, deprived the Plaintiffs and  
25

1 Class Members of such possession and use, and caused damages to the Plaintiffs and Class  
2 Members.

3 51. Plaintiffs and Class Members sought to maintain the secrecy and confidentiality  
4 of their Personal Information assets acquired by Defendant, which includes Personal Information  
5 (“PI”), Personally Identifiable Information (“PII”), Sensitive Identifying Information (“SII”),  
6 GPS “Fine” co-ordinates, derived in whole or part from linking their Unique Device Identifiers  
7 (“UDIDs”), to the Defendant OpenFeint user accounts, GPS “Fine” co-ordinates, and Facebook  
8 profile.  
9

10 52. The means by which Defendant obtained such information and the reasons  
11 Defendant engaged in its business practices made the basis of this action, demonstrate the  
12 confidential character of such information, users’ efforts to protect it, and the economic value of  
13 Plaintiffs’ and Class Members’ data.

14 53. Defendant’s conduct has caused economic loss to Plaintiffs and Class Members in  
15 that, in a barter economy in which users’ patronage (which is the subject of Defendant’s traffic  
16 measurement activities) is the currency with which users acquire ostensibly no-fee web services.  
17 Their patronage has independent economic value. In addition, inasmuch as Defendant  
18 wrongfully acquired Plaintiffs’ and Class Members’ patronage, Plaintiffs and Class Members  
19 were deprived of the opportunity to contribute their patronage to web entities that did not engage  
20 in such wrongful conduct.  
21

22 54. Further, the Plaintiffs’ and Class Members’ electronic data, misappropriated by  
23 Defendant, and populated with their actual user data constitute assets with discernable values.  
24 Certainly given Defendant conduct, Defendant associate economic value with the Plaintiffs’ and  
25 Class Members’ UDID derived data. In addition, they even have specific valuations in criminal  
26 markets. For example, Symantec reported that in 2007 the illicit market value of a valid Hotmail  
27  
28

1 or Yahoo cookie was three dollars (\$3.00).

2 55. The aggregated loss and damage sustained by Plaintiffs and Class Members,  
3 individually and collectively, set forth above includes economic loss with an aggregated value of  
4 at least \$5,000 during a one-year period. Defendant perpetrated the acts and omissions set forth  
5 in this complaint through an organized campaign of deployment, which constituted a single act.

6 56. Defendant's conduct, made the basis of this action, included acts of conversion  
7 whereby the Plaintiffs' and Class Members' mobile device data, which included sensitive and  
8 Personally Identifiable Information, was obtained by Defendant, exercising dominion over such  
9 property, and providing to third parties for commercial gain, including an economic loss to  
10 Plaintiffs and Class Members by the Defendant including but not limited to the following:

- 12 • Bandwidth is the amount of data that can be transmitted across a channel  
13 in a set amount of time. Any transmission of information on the internet  
14 includes bandwidth. Similar to utility companies, such as power or water,  
15 the "pipeline" is a substantial capital expenditure, and bandwidth usage  
16 controls the pricing model. Hosting providers charge users for bandwidth  
17 because their upstream provider charges them and so forth until it reaches  
18 the "back bone providers." Retail providers purchase it from wholesalers  
19 to sell its consumers.
- 20 • Network provider's data plans charge consumers based upon items, such  
21 items as usage and "caps." A charge of \$30.00 per month for an unlimited  
22 plan is standard, but limited plans have caps, such as: 256 GB per month.
- 23 • Defendant's tracking activity ads consume vast amounts of bandwidth,  
24 thereby slowing a user's internet connection by using their bandwidth.
- 25 • Advertisers are now using the internet as their primary ad-delivery pipe by  
26 continually uploading and downloading data from its networks causing  
27 substantial bandwidth use.

28 57. Defendant's conduct, made the basis of this action, resulted in an act of Trespass  
to the Personal Property/ Chattel of the Plaintiffs and Class Members by obtaining user data and  
a mobile device "Fingerprint," a practice of obtaining device information to perpetually identify  
the mobile device. The Defendant's actions were surreptitious, without notice and so were  
conducted without authorization and exceeding authorization. Defendant intentionally and

without consent, physically interfered with the use and enjoyment of personal property in the Plaintiffs' possession, thereby harming Plaintiffs and Class Members. The interference with the Plaintiffs' and Class Members' property/ chattel resulted in harm to their interest in the physical condition, quality or value of the property/ chattel.

58. Defendant OpenFeint's Terms of Service and Privacy Policy does not provide notice that users' mobile devices' UDIDs shall be obtained for tracking purposes, and used to build a profile data collected of any and all users' mobile device activities. Many Application Developers do not provide any Terms of Service and/or Privacy Policies.

59. If Plaintiffs and Class Members were adequately informed of Defendant OpenFeint's intrusive mobile tracking then they would not have enabled a mobile device application which was operated by Defendant OpenFeint.

### **FACTUAL ALLEGATIONS**

#### **A. Background**

60. "Kid Apps" are tracking millions of *Minor Children*, promoting "free" applications as a means to obtain their mobile device's UDIDs and Personally Identifiable Information, by attracting *minor children* with storybook tales, friendly animals and child-like game scenarios to create a mobile ecosystem similar to a "*virtual elementary school playground*." Many applications are being used as a ploy to obtain user's mobile device's UDIDs for financial gain. Defendant OpenFeint offers a mobile platform for applications to aggregate the user's mobile device UDIDs and Personal Identifiable Information obtained by applications, to link UDIDs to GPS "Fine" co-ordinates and to Facebook and/ or Twitter profiles.

61. In 1999, Intel released the "Pentium 3" and each processor included a unique serial number which could be read by software installed on the system. Intel was forced to remove this function after consumers, privacy groups, and legislative authorities voiced outrage

1 about privacy and security concerns. In 2008, Mobile Device Operating System Manufacturers  
2 started to include software with visible Unique Device Identifiers (“UDIDs”) within mobile  
3 devices. Coincidentally, Mobile Device Operating System Manufacturers also began developing  
4 application “stores” and “markets,” launched as a service for the operating system devices,  
5 permitting mobile device users to download applications.

6         62. Recent studies revealed that Mobile Device Operating System Manufacturers had,  
7 without authorization, transmitted, or allowed access to, UDIDs, permitting third parties to  
8 obtain mobile device users’ UDIDs. The “free” applications were being used as a tracking  
9 platform. Mobile Device Operating System Manufacturers, Advertising Networks, Web  
10 Analytics Vendors, Application Developers and Social Media affiliates; hereinafter referred to as  
11 the “Mobile Device Marketing Industry,” denied that obtaining a user’s mobile device’s UDIDs  
12 would permit mobile device tracking, and that user’s Personally Identifiable Information was  
13 being aggregated and linked to a user’s UDIDs, claiming UDIDs provided only “anonymous  
14 usage statistics.”  
15

16         63. Defendant OpenFeint is the largest mobile social gaming network, offering a  
17 mobile device platform that aggregates data; hereinafter referred to as a “Data Aggregator.”  
18 Defendant reports it is affiliated with in excess of five thousand three hundred (5,300) gaming  
19 applications involving one hundred million (100,000,000) users. Defendant OpenFeint  
20 aggregates data it obtains from users, provided in part by each of its affiliated applications.  
21 Defendant aggregates Personally Identifiable Information and links UDIDs to OpenFeint user  
22 accounts, linking UDIDs to GPS “Fine” co-ordinates (the user’s exact latitude and longitude),  
23 and linking UDIDs to Facebook and Twitter profiles, without notice or consent, to its users of its  
24 deceptive practices. Plaintiffs and Class Members are individuals that were harmed by Defendant  
25 OpenFeint.  
26  
27  
28



64. This consumer class action involves a pattern of covert mobile device surveillance; wherein the Defendant OpenFeint operated individually, and in concert with, associated in fact, Application Developers and Application Developer Affiliates that targeted Plaintiffs and Class Members who downloaded applications affiliated with Defendant OpenFeint to knowingly, and without the user's knowledge or consent, commit unauthorized transmittal, access, collection, and use of Plaintiffs' and Class Members' mobile device Unique Device Identifiers ("UDIDs"), to transmit a program, information, code, or command, to collect, monitor, and remotely store the Plaintiffs' and Class Members' aggregated Personally Identifiable Information link to their mobile device's UDIDs, in order to "track" the Plaintiffs and Class Members for financial gains.

65. Privacy and security concerns are further accentuated when it is known that Defendant OpenFeint implements GPS tracking involving "Fine" co-ordinates and that its acts are not limited to adults, but include *minor children*. Defendant OpenFeint targets *minor children* with free affiliated gaming applications designed and promoted as "*Kid apps*," purposely including storybook tales, friendly animals, and child-like game scenarios to attract *children*, so that the child's parents would be more likely to allow for the app download, relying in part on the posted *children app ratings*. Many of Defendant OpenFeint's gaming applications are rated 4+, for ages four (4) and up, rated 9+ for ages nine (9) and up, and rated 12+ for ages twelve and up.

66. Most Defendant OpenFeint affiliated applications provide no terms of service, privacy policy, or a link to a website with such information; moreover Defendant OpenFeint fails to provide a link to its terms of service or privacy policy within its platform. Many of the Defendant OpenFeint applications are marketed for *children 12 and under*. Defendant OpenFeint's platform allows forum postings, such as:

**Rated 4+ - (For Ages Four and Up)**

Patrick, *age 8*: “I love these jumps!!!”



***Rated 4+***

67. Defendant OpenFeint’s plug and play social gaming platform provides functionality for applications to attract “*Kiddies*”:

- “Social and mobile incubator YouWeb, who has helped create OpenFeint, (company names redacted), is announcing its latest venture..”
- “..an educational game and iPad app that combines scrolling gameplay dynamics with musical notes to get the *kiddies* interested in learning music.”
- “The game itself is using sister company OpenFeint’s plug and play social gaming platform to allows players to compare their scores and ranking with other players around the world.”

Leena Rao, “YouWeb Incubated Pluto Plays Music Combines Gaming With Helping Kids Learn Music,” May 12, 2011 (last accessed May 24, 2011) online: <http://techcrunch.com/2011/05/12/youweb-incubated-pluto-plays-music-combines-gaming-with-helping-kids-learn-music/>

68. The Intel Pentium 3 crisis pales in comparison to the privacy and security violations caused by Defendant OpenFeint’s platform and data aggregation of one hundred million (100,000,000) users, including *minor children*. However, Defendant OpenFeint can no longer claim the data is anonymous.

**B. Mobile Device Tracking**

69. Traditional online advertising practices, such as the tracking of individual users across sessions and controlling the frequency and relevance of advertising presented to them, simply do not exist in the mobile Internet today.

70. Mobile Internet advertising currently consists of streaming graphic files, in real

1 time, into content rendered by a user's mobile device browser. Image and text call to action  
2 advertising tags that are embedded in the content at a publisher's content management system.  
3 This occurs prior to delivery of the actual content to the user over the wireless network. Current  
4 mobile practice for many servers include ad serving systems to log delivery of user impressions  
5 when the ad tags are transmitted from the ad server, across the Internet to the publisher's content  
6 system.

7  
8 71. Mobile advertising systems lack reliable browser tracking while traditional online  
9 advertising relies on the user's browser cookies, implementations inherent in conventional  
10 implementations of mobile ad serving have effectively prevented mobile advertising from being  
11 effective.

12 72. The lack of standard advertising metrics for mobile campaigns has discouraged  
13 online advertisers from taking advantage of the unique personalized nature of mobile devices and  
14 local content. This is due in part from the inability of the mobile advertising industry to  
15 incorporate web analytics.  
16

17 73. There are basically two approaches to collecting web analytics data. The first,  
18 "page tagging," uses a small bit of JavaScript code placed on each web page to notify a third-  
19 party server when a page has been viewed by a web browser. Etags can be used in place of  
20 cookies. They are a part of caching in HTTP: The server sends the user the tag, and when the  
21 user accesses the resource again their web browser sends the tag back. The server uses the tag the  
22 browser sent to decide whether to send the user the data or provide data to the browser that the  
23 data hasn't changed, and to keep using the old copy.  
24

25 74. The second, and more traditional, approach to web analytics is "log file analysis,"  
26 where the log files that Web servers use to record all server transactions are also used to analyze  
27 website traffic.  
28

1           75. All Internet advertising, online or mobile, seeks “state maintenance” or the idea  
2 that the person/browser/phone that saw the ad performs some later activity. Because most mobile  
3 phones don’t support fully functional browsers, they also don’t obtain “uniqueness,” necessary to  
4 obtain “state maintenance.” Obtaining the user’s IP address won’t work because most mobile  
5 phones don’t have a public IP address. They access the web through Network Address  
6 Translation at the carrier, meaning that many phones are seen by the entire web as all one IP.

7  
8           76. In order to obtain “uniqueness” in mobile devices, the key was to obtain Unique  
9 Device Identifiers or “UDIDs,” a special type of identifier used in software applications to  
10 provide a unique reference number in mobile devices. Unlike traditional cookies, a user has no  
11 choice whatsoever here. A user can’t opt-out, since it is always sent. It can’t be deleted since it  
12 always stays the same. A user can not block UDIDs from being transmitted, as they would in a  
13 browser, since it is hard coded into a user’s phone software. Defendant OpenFeint accomplished  
14 the task of obtaining device uniqueness and reaped the benefits.

15  
16           77. With UDIDs, Application Developers were limited to a unique identifier,  
17 hereinafter referred to as a Global Unique Identifiers (“GUIDs”), which originates from a device  
18 registering at a website, online store, Web Analytic Vendors or by the ad networks. “GUIDs”  
19 created by Application Developers provides functionally that allows Application Developers to  
20 uniquely identify the user for purposes such as: storing application preferences or video game  
21 high scores, playlists, etc. In some cases, personal contact information and authorization to other  
22 linked accounts is also provided. This is so users don’t need to register or log on. GUIDs  
23 facilitated the process of collecting and storing certain types of data, but also provides a tempting  
24 opportunity for use as a tracking agent to correlate with other Personally Identifiable Information  
25 but GUIDs are not UDIDs, nor do they have the benefits of UDIDs.

26  
27           78. UDID tracking is not exactly comparable to any other type of tracking by  
28

1 advertising networks. It is not anonymous data – it is an exact ID that is unique to each physical  
2 device, and if merged with GPS data, it provides unlimited advertising opportunities. When  
3 tracking your location data on the mobile device, it is calculated to 8 decimal points that can be  
4 far more exact and accurate than any sort of geographically-based IP address look-up on the web.  
5 Instead of getting a general location, location data on a GPS-enabled mobile can identify your  
6 precise latitude and longitude.

7  
8 79. Advertising networks and mobile analytic companies obtain UDIDs to have  
9 visibility across all of its applications, so tracking is consistent regardless of an individual's  
10 location or connection. It is not anonymous tracking since it runs at the application layer, the  
11 same layer that a web-browser already runs; therefore its stats involve information which has  
12 nothing to do with user metrics or usage. Security violations occur when the device identifier is  
13 combined with the following attributes: authenticated login information (e.g. a banking  
14 application can link UDIDs with a full banking consumer profile), (nick)name of aOS device  
15 owner, type of connection (e.g. Wi-Fi versus 3G), model type (version of mobile device), home  
16 address, phone number, and geo-location information. While UDIDs' existence is not nefarious,  
17 its use can be.  
18

19 80. The advertising and marketing industries have been strongly advancing technical  
20 means of synchronizing tracking code so that information about individual consumer behavior in  
21 cyberspace can be shared between companies and the UDID used in the majority of mobile  
22 devices would be put to this purpose. The records of many different companies are merged  
23 without the user's knowledge or consent to provide an intrusive profile of activity on the  
24 computer. There are no practical limits on what can be collected or used.  
25

26 81. Many advertising and behavioral tracking systems that use UDIDs, without the  
27 customer's knowledge or consent, brag about its ability to report on every action a user took  
28

1 within an app: every button click, every page viewed, every table cell viewed, and the time a  
2 person took between each action, all sent back to the server without any notification or customer  
3 access to that information. Thus, UDIDs are most useful to people who want to track and collect  
4 user behavioral data without user notification or permission (ad networks and behavioral  
5 monitors). Since UDIDs are the same for every app on a device, this is a benefit to advertisers  
6 and other data aggregators. The mobile advertising world will no longer have to place a cookie to  
7 track a user across sites/apps because UDIDs are like a permanent cookie that the user cannot  
8 turn off.  
9

10 82. Application Developers and Application Developers Affiliates' technology, made  
11 the basis of this action, is basically using some of the modern HTML5 capabilities of mobile  
12 browsers to perform the same tasks as a traditional cookie, but out of sight of most users and  
13 while it is not technically a mobile cookie since it's not browser based, is on the server side, thus  
14 it cannot be affected by anti-cookie technologies employed by carriers such as gateway stripping  
15 (a technique that renders the cookies useless or unreliable for ad targeting), and preventing users  
16 from deleting them. Wireless carriers typically prevent outside firms from embedding such  
17 information in mobile devices. In order to get around the carriers, it embeds its digital code in  
18 servers rather than browsers, since most mobile devices forbid the use of third party software in  
19 Applications to collect and send Device Data to a third party for processing or analysis, banning  
20 "Third Party" Analytics.  
21

22 83. In a non-technical version, Application Developer's Affiliates have its  
23 Application Developers include a small JavaScript in its application. An invisible iFrame is  
24 created which loads code from the application. It determines if it has seen the user before and  
25 initiates a database (for the domain) and then communicates through iFrame message-passing to  
26 its client that it should create a mirror of this database for the application domain.  
27  
28

1           84.     Application Developer's Affiliates develop and sell tools to track, collect (and  
2 store) data and analyze mobile and Internet-enabled apps to facilitate advertising or assist  
3 developers build applications. In the final analysis, the developer/application publisher should  
4 also be held responsible for any and all data privacy violations.

5           85.     By piggy backing on applications, Application Developer's Affiliates gain access  
6 to the richest customer metrics with the shortest distance to customer purchase decisions and the  
7 sales funnel. Web analytic vendors track app usage, but also attract advertisers for third-party  
8 applications and Application Developer's Affiliates service itself. In addition to ad-insertion  
9 technology, the web analytics vendor is involved in the ad network. Mobile analytics' purpose is  
10 an optimization tool to help increase app downloads and sales.

12           86.     Developing an account creation system is time consuming and costly. Therefore,  
13 in order to save time and money, the majority of Application Developers who do not need multi-  
14 device accounts choose to use UDIDs instead of its own GUIDs. As such, Defendant OpenFeint  
15 incentivizes developers to use the UDID by not providing them with a similarly useful privacy-  
16 enhanced customer identification tool. Privacy risks associated with the use of UDIDs could  
17 have been mitigated by Defendant OpenFeint by using an identifier that was unique for the  
18 combination of application and device if the device returned to a program different for each app.

20           87.     Application Developer's Affiliates offer "free" software development kits  
21 (hereinafter referred to as "SDKs") that Application Developers download and insert into its  
22 application. A software development kit ("SDK") is typically a set of development tools that  
23 allows for the creation of applications for a certain software package, software framework,  
24 hardware platform, computer system, video game console, operating system, or similar platform.  
25 It may be something as simple as an application programming interface (API), in the form of  
26 some files, to interface to a particular programming language or include sophisticated hardware  
27  
28



1 to communicate with a certain embedded system. Often SDKs can be downloaded directly via  
2 the Internet. Many SDKs are provided for free to encourage Application Developers to use the  
3 Application Developer Affiliates system or language.

4 88. The spectrum of mobile analytics involves: “application analytics” aimed at  
5 Application Developers; “campaign analytics” aimed at optimizing tools for media companies;  
6 and “service analytics” aimed at providing platforms for data mining networks or mobile device  
7 data.

8  
9 89. SDKs though provided Application Developer Affiliates the access to Application  
10 users when Application Developers downloaded the Application Developer Affiliates’ SDKs  
11 into its application; such provided the ability to obtain the Plaintiffs’ and Class Members’ UDID  
12 and to conduct cross application tracking, activities made the basis of this action.

13 90. The SDKs also involve tracking libraries, whose sole purpose is to collect and  
14 compile statistics on application uses and usage, and send the device ID as part of their  
15 functionality. Most of these libraries are used to display advertisements so as to provide revenue  
16 for the Application Developer; and the mechanism for the libraries to also provide the mobile  
17 device’s UDID once the user installed applications.

18  
19 91. The SDKs enable Application Developers to track usage of its app in real time, as  
20 if it were a website. First, the Application Developer identifies the places in its app where it  
21 would like to trigger a page view or an event, and then uses the SDKs to send these events to  
22 Web Analytics Vendors.

23  
24 92. Client libraries available for Applications were created using open source SDKs  
25 for consistency and easy integration. The client libraries also provide flexibility for deeper  
26 integrations and customization. Once integrated with an app, the client library sends function  
27 calls (Required: open, upload, close. Optional: tagEvent, setOptIn / isOptIn) to control a session.

1 These calls to the server can be uploaded upon start of the application (recommended) to place  
2 one single server call with batched information or it can be configured to fire more or less  
3 frequently. Analytic data is written to persistent storage immediately after its recorded and is  
4 available within the user interface in real-time.

5 93. Essentially, Web Analytics consist of a library that is compiled into an application  
6 and a web service. Generally when the application starts, it pings the web service with a small  
7 amount of information and when the application is about to terminate, it pings the service again.  
8 The developer may also choose to ping the service at other various points in the application.  
9 These pings are then aggregated on the server into various reports. The UDIDs will also be sent  
10 in the ping so they know what app to count the ping on.  
11

12 94. UDIDs without user's mobile device data may not be linked directly to a user;  
13 however "Libraries" of data exist, such as Facebook where an Application Developer can use  
14 such to integrate Facebook library with the apps thus connecting the user's UDIDs to the user.  
15 The Facebook connect on the application allows the app developer to obtain a Facebook ID, once  
16 a user is logged in, and then the app developer can link UDIDs to a Facebook account in order to  
17 link a user to a mobile device.  
18

19 95. Game app developers, using user's high scores, can also be tracked if UDIDs are  
20 obtained from a mobile device and related to an application in addition to relying on UDIDs.

21 96. Application Developers Affiliates collect mobile device data, including the user's  
22 UDIDs, to aggregate such into a variety of reports, merging data from all associated applications,  
23 to produce reports by price point, application category, operating system and various other  
24 criteria. The aggregated data is then impossible to determine which application data supplied the  
25 specific processor data.  
26  
27  
28

1           **C. UDIDs Tracking Studies**

2           97.     Mobile tracking entities attempt to claim their transactions are anonymous and  
3 thoroughly randomized. However, recent studies exposed those mobile tracking entities’  
4 business practices with Application Developers, Advertising Networks, and Web Analytic  
5 Vendors, such as those associated with Defendant OpenFeint, do not confirm this opinion.

6           98.     On September 28, 2010, a joint study by Intel Labs, Penn State, and Duke  
7 University was released. The study identified that publicly available cell-phone applications from  
8 application markets were releasing consumers’ private information to online advertisers. In a  
9 study of 30 popular applications, TaintDroid revealed that 15 applications send users’ geographic  
10 location to remote advertisement servers. The researchers were only able to monitor Android  
11 apps because its operating system is an open source. That allowed them to develop TaintDroid,  
12 software that labels, or taints, data from privacy-sensitive sources so it can be monitored in real  
13 time. The study also found that seven of the 30 applications send a unique phone (hardware)  
14 identifier.  
15

16           •       “Our experimentation indicates these fifteen applications collect location data and  
17 send it to advertisement servers. In some cases, location data was transmitted to advertisement  
18 servers even when no advertisement was displayed in the application.”  
19

20 William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick  
21 McDaniel, Anmol N. Sheth, “TaintDroid: An Information-Flow Tracking System for Realtime  
22 Privacy Monitoring on Smartphones” (last accessed May 25, 2010), online:  
<http://www.appanalysis.org/tdroid10.pdf>

23           99.     On October 1, 2010, a second study written by Eric Smith, Assistant Director of  
24 Information Security and Networking at Bucknell University, raised similar privacy questions  
25 about how Unique Device Identifiers (“UDIDs”) could be used to track how customers use  
26 applications associated with the device, and how developers can access a device UDID and  
27 correlate it with Personally Identifiable Information:  
28

- “A number of applications which have the potential to map UDID to user identity were studied to determine if they are actively collecting UDID data. UDID collection by applications requesting user credentials. Of the applications evaluated in this study that collected UDIDs require users to log in, and have personally-identifiable information affiliated with user accounts, 30% clearly transmit UDIDs; the rest used SSL to encrypt data transmission.”
- “Of those, 68 percent transmitted UDIDs to servers under the control of developers or advertisers, while another 18 percent sent encrypted data that could have included the unique serial number. Just 14 percent of the apps were confirmed not to send UDIDs.”
- “It is clear from this data that most mobile device application vendors are collecting and remotely storing UDID data, and that some of these vendors also have the ability to correlate the UDID to a real-world identity.”
- “A number of the applications considered in this study requested access to the on-board GPS receiver. Several such applications – games, for example -- had no obvious need for this information. In several cases, applications which transmitted UDIDs were observed to transmit the mobile device’s latitude and longitude as well.”

Eric Smith, “iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)” (last accessed May 25, 2010), online: <http://www.pskl.us/wp/wp-content/uploads/2010/09/Android-Applications-Privacy-Issues.pdf>

100. On December 17, 2010, a third study by David Campbell and Ashkan Soltani revealed that OpenFeint application were transmitting UDIDs:

- “An examination of 101 popular smartphone “apps”—games and other software applications for Android and Android phones—showed that 56 transmitted the phone’s unique device ID to other companies without users’ awareness or consent. Forty-seven apps transmitted the phone’s location in some way. Five sent age, gender and other personal details to outsiders.”
- “Many apps don’t offer even a basic form of consumer protection: written privacy policies. Forty-five of the 101 apps didn’t provide privacy policies on their websites or inside the apps at the time of testing. OpenFeint requires app privacy policies to?”

David Campbell and Ashkan Soltani, Electric Alchemy.net, “The Journal’s Cellphone Testing Methodology,” (last accessed May 25, 2011), online: <http://online.wsj.com/article/SB10001424052748704034804576025951767626460.html>

1           101. On January 24, 2011, a fourth study by the Vienna University of Technology,  
 2 Austria was released which confirmed previous studies that Android applications were obtaining  
 3 UDIDs:

- 4           • “To show the feasibility of our approach, we have analyzed more  
 5 than 1400 Android applications. Our results demonstrate that a  
 6 majority of application leak the device ID.”
- 7           • “While not directly written by an application developer, libraries  
 8 that leak device IDs still pose a privacy risk to users. This is  
 9 because the company that is running the advertisement or statistics  
 10 service has the possibility to aggregate detailed application usage  
 11 profiles. In particular, for a popular library, the advertiser could  
 12 learn precisely which subset of applications (that include this  
 13 library) are installed on which devices. For example, in our  
 14 evaluation data set, AdMob is the most-widely-used library to  
 15 serve advertisements. That is, 82% of the applications that rely on  
 16 third-party advertising libraries include AdMob. Since each request  
 17 to the third-party server includes the unique device ID and the  
 18 application ID, AdMob can easily aggregate which applications are  
 19 used on any given device.”
- 20           • “Obviously, the device ID cannot immediately be linked to a  
 21 particular user. However, there is always the risk that such a  
 22 connection can be made by leveraging additional information. For  
 23 example, AdMob was recently acquired by OpenFeint. Hence, if a  
 24 user happens to have an active OpenFeint account and uses her  
 25 device to access OpenFeint’s services (e.g., by using Gmail), it  
 26 now becomes possible for OpenFeint to tie this user account to a  
 27 mobile phone device. As a result, the information collected  
 28 through the ad service can be used to obtain a detailed overview of  
 who is using which applications. Similar considerations apply to  
 many other services (such as social networks like Facebook) that  
 have the potential to link a device ID to a user profile (assuming  
 the user has installed the social networking application). The  
 aforementioned privacy risk could be mitigated by OpenFeint if an  
 identifier would be used that is unique for the combination of  
 application and device. That is, the device ID returned to a  
 program should be different for each application.”
- “The unique device ID of the phone is treated differently and more  
 than half of the applications leak this information (often because of  
 advertisement and tracking libraries that are bundled with the  
 application). While these IDs cannot be directly linked to a user’s  
 identity, they allow third parties to profile user behavior.  
 Moreover, there is always the risk that outside information can be  
 used to eventually make the connection between the device ID and

a user.”

Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna, “PaOS: Detecting Privacy Leaks in aOS Applications” (last accessed May 25, 2011), online: <http://www.iseclab.org/papers/egele-ndss11.pdf>

#### **D. OpenFeint**

102. Defendant OpenFeint presents itself as a standalone application providing a “social platform” for mobile devices and allowing Application Developers to add social networking aspects into their gaming applications, providing access to leaderboards, geo-location leaderboards, achievements, cloud storage for saved games, online presence and instant messaging, in-app forums, social discovery of games, friending, favorite games lists, Facebook connect integration with photo import and status updates, twitter integration, social challenges, push notifications, cross-promotion, a user interface, social game recommendations, game-specific information, and general settings. Defendant OpenFeint is essentially a mobile platform to obtain user’s UDIDs, aggregate user’s data, and sell such for financial gains.

103. Defendant OpenFeint’s predecessor, Aurora Feint, is no stranger to user tracking without notice or consent, and its actions were similar in nature to Defendant OpenFeint’s business model. In 2008, Aurora Feint was involved with privacy concerns and suspended from a mobile app store. Users that opted to the community feature had Aurora Feint obtain a user’s contact list, send it unencrypted to its servers, and match a user with their friends who were currently playing games:

“When we discovered that the Apple SDK allowed us to look through your contact list we thought it would be a great idea to automatically show you which friends are playing the game. why automatically? Well, everyone always complains about the keyboard on the iPhone and how annoying it is to type on it. so we thought, "hey, why don't we make this feature really easy to use – no typing!" And such, the community feature was born. Some people have said that it would have been ok if we had a better notice explaining what was going on. I agree! We weren't trying to be sneaky about how this worked. It was just overlooked. No one we showed it to even asked a question about it – nor did we. It just simply never came up as a potential issue when we beta tested the game with

early users.”

Jason Chen “Aurora Feint iPhone App Delisted For Lousy Security Practices” June 23, 2008, (last accessed May 28, 2011) online: <http://gizmodo.com/5028459/aurora-feint-iphone-app-delisted-for-lousy-security-practices>

104. The Defendant OpenFeint is aiming to do the same thing for mobile in-game purchases that was done for computer based games: provide developers with a free set of tools to implement important features without the cost of managing these elements themselves. By using the “OpenFeint SDK,” mobile game developers can transform traditional stand-alone mobile games into interactive social online games, cross-promote their games, eventually monetize users with the sale of virtual goods and virtual currency, display advertisements, and include additional revenue-making activities.

105. Defendant OpenFeint’s platform creates a central network for “gamers” to incorporate social networking capabilities, allowing the ability to import friends from a user’s Facebook and/ or Twitter profile so as to leverage social networking services. Application Developers integrate Defendant OpenFeint platform because it adds a social layer to their apps allowing access to Facebook and Twitter profile pages, Facebook-like walls for others to write on, and the ability to chat in games. OpenFeint works as a ‘layer’ on top of the actual game using a multi-layered interface. OpenFeint enabled games have the option of including a badge on the corner of the game’s icon consisting of the OpenFeint logo, initially visible to the user after they begin to download applications.

106. Mobile Device Operating System Manufacturers developed application programs which are preinstalled on most devices and allow users to browse and download apps published by third-party developers. Users downloaded the applications which then provided access to Defendant OpenFeint.

107. The “Android Market” is a mobile application site developed by Google for Android devices, and the “iTunes Store” was developed by Apple to provide apps for mobile



1 devices; hereinafter collectively referred to as the “App Markets.” Defendant OpenFeint provides  
 2 a platform for both the iTunes Store and Android Market applications; hereinafter referred  
 3 collectively to as the “OpenFeint Platform.”

4 108. Mobile devices run applications written by third-party developers and distributed  
 5 through the App Markets. Once developers have signed up, they can make their applications  
 6 available immediately without a lengthy approval process. When an application is installed, the  
 7 App Markets display all required permissions. The user can then decide whether to install the  
 8 application based on those permissions. The user may decide not to install an application whose  
 9 permission requirements seem excessive or unnecessary, i.e. a game may need to enable  
 10 vibration, but few applications would have any plausible reason to access a user’s “Fine”  
 11 location GPS, which refers to the user’s exact location and latitude. Possible app permissions  
 12 include functionality such as:

- 14 • Accessing the Internet
- 15 • Making phone calls
- 16 • Sending SMS messages
- 17 • Reading and writing to the installed memory card
- 18 • Accessing a user’s address book data

19 109. The application’s implementation details are self-contained Package files. Neither  
 20 the App Markets, nor the OpenFeint platform install applications itself, rather the phone’s  
 21 Package Manager Service installs the applications. The package manager can be seen directly if  
 22 the user tries to download an APK file directly to their phone. Applications can be installed to  
 23 the phone’s internal storage, and can also be installed to the owner’s external storage card.

24 110. Application Developers must initially obtain an OpenFeint certification that its  
 25 App complies with OpenFeint’s developer policies. The OpenFeint’s platform stresses that it  
 26 requires an approval for process Application Developers to have their applications listed. In all  
 27 actuality though, Defendant OpenFeint platform fails to screen its Apps.

28 111. Defendant OpenFeint’s platform provides a Software Developer Kit (“SDK”) that

1 allows the apps the ability to import the tracking code into apps to track Plaintiffs and Class  
2 Members' mobile device activity. The OpenFeint Software Development Kit License Agreement  
3 and its Terms and Conditions provide assurances to Plaintiffs and Class Members of OpenFeint's  
4 contractual obligation to protect the privacy and security of its Users.

5 112. Defendant OpenFeint's "sandboxing mechanism", a technique to create a  
6 configured execution environment, attempts to limit access to other application data by  
7 preventing third party applications from seeing each other or accessing specific locations;  
8 however such prevention serves no purpose when Defendant combines the UDIDs and mobile  
9 device data derived from the sandboxing mechanism.  
10

11 113. Ad Networks and Web Analytics Vendors are associated with a multitude of  
12 Defendant OpenFeint applications and are thus able to cross-track user's mobile devices,  
13 accessing the user's UDIDs, making it possible to track users even when they change their  
14 device.  
15

16 114. The device unique identifier is obtained through the Defendant OpenFeint's  
17 SDK's API. It may be used to aggregate data collected from various applications and analytics  
18 frameworks. Applications are able to know which other applications users have added and  
19 implemented. Users are now having their computer's unique identifier transmitted to Ad  
20 Networks and Web Analytics vendors, without their notice or consent.

21 115. While Mobile Device Operating System Manufacturers requires its apps to notify  
22 users before they download the app regarding the data sources the app intends to access, it does  
23 not gently require apps to ask permission to access some forms of the device's IDs, or to send it  
24 to third parties. When smartphone users let an app see their location, apps generally don't  
25 disclose if they will pass the location to ad companies, thus avoiding the manifest file. From an  
26  
27  
28

1 advertiser perspective, the ID-related data collection enables the tracking and optimization of  
2 mobile ad campaigns.

3 116. The Mobile Device Operating System Manufacturers is therefore used to  
4 obfuscate the privacy and security settings of the user's mobile device, such as the Application  
5 Developer's ability to write code to get the MAC address of the phone. Multiple applications  
6 from that same developer can also send the same UDID to the developer's servers. Mobile  
7 device operating system manufacturers do not provide controls to adequately protect users'  
8 sensitive data.  
9

10 117. Mobile device operating system manufacturers require permission be granted by  
11 the user to allow applications access to *some* specific types of user data, but not *all*. The current  
12 model where permissions are granted to applications combined with the way third party libraries,  
13 such as mobile ad network libraries, request many different types of information which sets up a  
14 situation where the ad network will get the information if the application needs it to operate.  
15

16 118. Application Developers must initially register their applications on  
17 Api.openfeint.com and may add OpenFeint as either a framework or an individual source file.  
18 Defendant OpenFeint's Developer Dashboard is the center of activity for developers working  
19 with Defendant OpenFeint. From here they will create their free developer account, download  
20 the Defendant OpenFeint SDK, and manage server side components of their projects. Defendant  
21 OpenFeint's source code, a static framework, is released under the Terms of the GNU Lesser  
22 General Public License, which does not allow static linking, while Mobile Device Operating  
23 System Manufacturers forbid dynamic linking. Defendant OpenFeint's framework includes, but  
24 is not limited to, the following:  
25

- 26 a. libsqlite3.0.dylib
- 27 b. AddressBook
- 28 c. AddressBookUI

d. CoreLocation

e. Mapkit

f. Libz .1.2.3. dylib

119. Any application affiliated with Defendant OpenFeint will initially provide a pop-up requesting the user enable Defendant OpenFeint. If such is authorized, then there is a pop-up enabling Defendant OpenFeint geo-location before the application being downloaded requests access to geo-location. Mobile Device Operating System Manufacturers have strict guidelines it provides to applications that request the user's geo-location. Defendant OpenFeint was not permitted by Mobile Device Operating System Manufacturers to obtain the user's geo-location in lieu of the applications.

120. A common flow of events when a user first starts an OpenFeint-enabled application is as follows:

1) An OpenFeint screen pops up, prompting an account for the user to log in.

2) On the same screen, there is an option the user can select to configure OpenFeint to use location data or not.

3) If the user elects to allow OpenFeint to use location data, OpenFeint will attempt to access the user's location. At this point, the user will be prompted to allow the application to access their location data. The reason for this two-step process is that the device considers the application and OpenFeint to be one and the same entity.

121. Mobile device operating system manufacturers generally collect 30%, of app purchases and the Application Developer divides the remaining 70% with Defendant OpenFeint, of which Defendant OpenFeint receives 15% on paid apps. Defendant OpenFeint's "One Touch iPromote," gives users the ability to find and buy other OpenFeint-supported games their friends are playing, inviting other users into "lobbies," where everyone can see what everyone else is playing. A user can then decide to play the same game or click on the link to buy it. One touch

iPromote is based on revenue sharing. When a user clicks on a game in a lobby and then goes on to buy that game, the developer and Defendant OpenFeint will get a percentage of that sale. Defendant OpenFeint wants user's transactions and funds to occur within the Defendant OpenFeint interface as opposed to strictly within the App Markets. For app developers, the tradeoff is the benefit of not having to create complex art assets or a storefront design. Instead, they will just be able to include it with all the other OpenFeint plug-ins.

OpenFeint, OpenFeint Developers site, Last Updated: April 19, 2011(last accessed May 25, 2011), Online: <http://support.openfeint.com/dev/ofx-billing-faq/>

#### **E. OpenFeint Tracking**

122. When studies revealed in 2010 that Mobile Device's Operating Systems were "leaking" user's UDIDs to third parties by using the "free" downloaded apps as a ploy to draw a user base and the app platform as a routing port to conduct these activities, the mobile marketing industry downplayed the significance of the findings by claiming such was "anonymous" and that user's Personally Identifiable Information was not being linked to the user's UDIDs. Since the studies only revealed the source of the "leak" and its destination, there was no research that revealed the mobile industry's actual business practices of aggregation of user's data and the process of linking user's Personally Identifiable Information *after* the user's UDIDs were obtained until the recent "Cortesi Study."

123. Cortesi examined the Application Programming Interfaces (API) and the data that was passed back and forth, specifically concentrating on Unique Device Identifier (UDIDs) and how it could be associated (or "linkable") to other identifying data sets. UDIDs by itself don't expose personal data, but to the extent that it's linked to other information about the mobile device's user, it can function like a permanent cookie used in non-mobile tracking. Cortesi demonstrated a "linkability" between UDIDs and GPS co-ordinates, exposing a geo-location privacy risk to the person who carries the device, and a linkability to

Facebook and/ or Twitter profiles and profile pictures:

- “The most common destination for traffic containing a user’s UDID is Apple itself, followed by the Flurry mobile analytics network and *OpenFeint*, a mobile social gaming company. These companies are uber-aggregators of UDID-linked user information, because so many apps use their APIs.
- When an OpenFeint-enabled app is first fired up, it submits the device's UDID to OpenFeint's servers, which then return a list of associated accounts: [https://api.openfeint.com/users/for\\_device.xml?udid=XXX](https://api.openfeint.com/users/for_device.xml?udid=XXX)
- This is a completely unauthenticated call - you can try it out by cutting and pasting it into your browser, replacing XXX with your own UDID. Here's an example of the response for my UDID, with sensitive information removed:

```
<?xml version="1.0" encoding="UTF-8"?>
<resources>
  <user>
    <chat_enabled>true</chat_enabled>
    <gamer_score>XXX</gamer_score>
    <id>XXX</id>
    <last_played_game_id>187402</last_played_game_id>
    <last_played_game_name>tiny wings</last_played_game_name>
    <lat>XXX</lat>
    <lng>XXX</lng>
    <online>false</online>

    <profile_picture_source>FbconnectCredential</profile_picture_source>
  >
    <profile_picture_updated_at>XXX</profile_picture_updated_at>
    <profile_picture_url>http://XXX>
    <uploaded_profile_picture_content_type nil="true">
    </uploaded_profile_picture_content_type>
    <uploaded_profile_picture_file_name nil="true">
    </uploaded_profile_picture_file_name>
    <uploaded_profile_picture_file_size nil="true">
    </uploaded_profile_picture_file_size>
    <uploaded_profile_picture_updated_at nil="true">
    </uploaded_profile_picture_updated_at>
    <name>XXX</name>
  </user>
</resources>
```

Included is my latitude and longitude, the last game I played, my chosen account name, and my Facebook profile picture URL.

### Linking UDIDs to GPS co-ordinates

1 If the user has opted to allow OpenFeint to use their location, latitude and  
 2 longitude is returned in the profile results. This lets us trivially associate a  
 UDID with GPS co-ordinates.

3 *The location leak was fixed by OpenFeint after my report. Although some*  
 4 *portions of the OpenFeint API still returns a user location, it seems that it*  
*is no longer served for direct profile requests.*

### 5 **Linking UDIDs to Facebook profiles**

6 If the user registered a Facebook account with OpenFeint, a profile picture  
 7 URL hosted by the Facebook CDN was returned in the user's profile data.  
 8 Facebook profile picture URLs include the user's Facebook ID, directly  
 linking it to their Facebook account.

9 This step represents a complete de-anonymization of the UDID, directly  
 10 linking the supposedly anonymous identifier with a user's real-world  
 identity.

11 *The Facebook ID leak was fixed by OpenFeint after my report.*

### 12 **OpenFeint's response**

13 I reported this problem to OpenFeint on 5th of April. I did not hear back  
 14 from them immediately, but I knew they were working on the problem  
 15 because their API stopped returning GPS coordinates and Facebook  
 16 profile picture URLs. On the 12th, I received an email from Jason Citron,  
 17 OpenFeint's CEO, who wanted to set up a phone conversation with me,  
 18 him and an OpenFeint legal representative. We spoke on the evening of  
 19 the 20th of April. I recapped my findings and expressed concern that their  
 20 API still linked UDIDs to user accounts. They thanked me for the  
 vulnerability report, confirmed that they had tightened their API in  
 response to it, and asked for more time to consider the issue before I  
 released anything. The following morning, it was announced that  
 OpenFeint had been bought by GREE for \$104 million.

### 21 **Impact**

- 22 • I was able to link roughly 30% of UDIDs to GPS co-ordinates, 20% of  
 23 users to a weak identity (e.g. OpenFeint profile picture, user-chosen  
 account name), and 10% of UDIDs directly to a Facebook profile.
- 24 • We can make a broad guess at the magnitude of the problem, based on the  
 25 fact that OpenFeint claims to have 75 million users: This would mean that  
 26 about 7.5 million users may have had Facebook accounts linked publicly  
 to their UDIDs until OpenFeint stopped returning profile picture URLs a  
 few weeks ago.
- 27 • About 22.5 million users may have had GPS co-ordinates linked publicly  
 28 to their UDIDs until the issue was corrected.



- 1 • About 15 million users may still have identifying information like profile  
2 pictures and user-chosen account names (that can often be used to identify  
3 users) exposed.
- 4 • All 75 million users still have personal details like the last OpenFeint-  
5 enabled game they played and whether they are online (i.e. logged in to  
6 the OpenFeint network) exposed.
- 7 • Although the Facebook and GPS de-anonymization issues have been  
8 repaired, we have to consider the possibility that these vulnerabilities have  
9 already been used to de-anonymize a database of UDIDs.

### 10 **Conclusion**

11 UPDATE: OpenFeint says that upon learning of the vulnerability it  
12 immediately stopped transmitting location and disabled the use of  
13 Facebook for profile pictures on the service.”

14 Aldo Cortesi, “De-anonymizing Apple UDIDs with OpenFeint,” May 4, 2011 (last accessed  
15 May 28, 2011), online: [http://corte.si/posts/security/openfeint-udid-](http://corte.si/posts/security/openfeint-udid-deanonymization/index.html)  
16 [deanonymization/index.html](http://corte.si/posts/security/openfeint-udid-deanonymization/index.html)

#### 17 **1. Linking UDIDs to OpenFeint User Accounts**

18 124. Plaintiffs and Class Members were not provided adequate notice, nor consented  
19 to, Defendant OpenFeint linking their mobile device’s UDIDs to their OpenFeint user’s  
20 accounts.

21 125. To understand why linking UDIDs to Defendant OpenFeint user accounts is a  
22 privacy and security crisis, an analysis of how UDIDs are used in the broader Application  
23 ecosystem is needed. The noted studies revealed that the vast majority of applications send  
24 UDIDs to servers on the Internet and that UDID-linked user information is aggregated in literally  
25 thousands of databases on the net. In this context, UDIDs de-anonymization links connect all  
26 mobile actions and transactions to a user’s Personally Identifying Information causing privacy  
27 and security risks and violations. Once the Defendant OpenFeint SDK’s software bundle obtains  
28 the user’s UDIDs, it then sends the UDIDs “upstream” to the OpenFeint servers. First, the UDID  
is obtained from the mobile device itself through a mobile device operating system manufacturer  
created API; therefore UDIDs are obtained from the mobile device without external

1 communication. Second, and more importantly, the Mobile Device Operating System  
 2 Manufacturers' permissions structure does not distinguish between the application and  
 3 OpenFeint; it is all seen as one unit.

4 126. Traditional online advertising does not obtain user's mobile devices UDIDs.  
 5 Defendant OpenFeint's objective was to obtain a mobile device's "Fingerprint," a practice of  
 6 obtaining mobile device information to perpetually identify the mobile device as identification,  
 7 which can then be linked to additional data elements to identify "Personally Identifiable  
 8 Information" ("PII"), Personal Information and/ or Sensitive Information:  
 9

10 *"If we ask whether a fact about a person identifies that person, it turns out*  
 11 *that the answer isn't simply yes or no. If all I know about a person is their*  
 12 *ZIP code, I don't know who they are. If all I know is their date of birth, I*  
 13 *don't know who they are. If all I know is their gender, I don't know who*  
 14 *they are. But it turns out that if I know these three things about a person, I*  
 15 *could probably deduce their identity! Each of the facts is partially*  
 16 *identifying."*

17 Electronic Frontier Foundation, Technical Analysis by Peter Eckersley, "A Primer on  
 18 Information Theory and Privacy" (last accessed April 15, 2011), online:  
 19 <http://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy>

20 127. Defendant OpenFeint's SDK is downloaded within the client application by the  
 21 Application Developer; however it is not known whether such occurs *before* or *after* it is  
 22 submitted to the App Markets for review. The review may not include Defendant OpenFeint's  
 23 SDK that contains tools and codes for Application Developers use that are not included in the  
 24 distributed apps.

25 128. The use of mobile device identifiers linked to specific user data concerns 87% of  
 26 all Americans who can be uniquely identified if date of birth, gender and geographic location is  
 27 known.

28 *"Uniqueness of Simple Demographics in the U.S. Population by: Latanya*  
*Sweeney. LIDAP-WP4 Carnegie Mellon University, Laboratory for*  
*International Data Privacy, Pittsburgh, PA: 2000 (1000)"*

129. Defendant OpenFeint's API is split into two parts. The first is entirely

1 unauthenticated; the second is authenticated with the credentials of the Application Developer.  
2 After the Cortesi Study, the unauthenticated part of OpenFeint's API stopped returning latitude  
3 and longitude that could be viewed by analyzing unauthenticated credentials. Without the ability  
4 to analyze the latitude and longitude obtained, the application's authenticated credentials were  
5 now provided to Defendant OpenFeint. There still exists a need for the user to inspect the traffic  
6 from their mobile device during normal use to determine whether the authenticated portions of  
7 Defendant OpenFeint's API do still return latitude and longitude for other users (for example,  
8 "friends" of the current user) obtaining a latitude and longitude for an arbitrary user.  
9

10 130. Mobile Device Operating System Manufacturers that operate the App Markets  
11 explicitly tell Application Developers that they must not publicly associate a mobile device's  
12 unique identifier with a user account to ensure privacy. Mobile Device Operating System  
13 Manufacturers make the UDIDs available through an API call, originated from the application,  
14 only after the application has been screened and provided contractual assurances that it will abide  
15 by the App Market's Terms of Licensing Agreement. However, Defendant OpenFeint was not a  
16 party to this original Licensing Agreement. Defendant OpenFeint SDK's software bundle was  
17 not included in the Mobile Device Operating System, nor the approved app, as such the Mobile  
18 Device Operating System Manufacturers that operate the App Markets allowed only the  
19 applications to use its API call to access the user's UDIDs.  
20

21 131. Both parts of Defendant OpenFeint's API are intended for use by OpenFeint  
22 applications, but because of the way they designed their protocols, one part of it has no  
23 authentication. "Deeper" parts of the API can be authenticated using the app developer's  
24 credentials (i.e. using the same credentials for all installed instances of the app), and supported  
25 by observing the traffic flowing to and from a user's phone in motion.  
26

27 132. OpenFeint does not have a contract with the Mobile Device Operating Service  
28

Manufacturers to access any of the mobile device data that is permitted by the applications. Defendant OpenFeint must use its SDK to circumvent the security protections created by the Mobile Device Operating System Manufacturers.

133. The largest risk is that OpenFeint is returning all of this data unauthenticated. Third parties can query, based on UDIDs, and obtain this information. A user's information is exposed on the internet and therefore a huge privacy risk. Moreover, Defendant OpenFeint "hogs" the Plaintiffs' and Class Members' bandwidth to conduct its unauthorized marketing practices:

- 84% of apps tested contacted one or more domains during use. At the extreme end, iDestroy contacted 14 domains, including 3 different ad networks and OpenFeint.
- 74% of apps tested sent the device UDID to one or more domains.
- 46% of apps that transmitted UDIDs did so in the clear.
- 54% of apps transmitting UDIDs used encryption for all UDID traffic.

Aldo Cortesi, "How UDIDs are used: a survey" May 19, 2011 (last accessed May 29, 2011) online: <http://corte.si/posts/security/apple-udid-survey/>

134. An additional privacy risk is when the data goes "upstream" from OpenFeint servers - only OpenFeint knows where the data goes after it hits their databases. Defendant OpenFeint provides "cloud storage" for data by using "The OpenFeint Network Save Card service," and providing a simple API that enables an application to save a "blob" of data to the server and retrieve it later. Each blob is associated with a specific application, a specific user, and a key name chosen by the application. An application can only access blobs that it has created and only those that are associated with the current user. OpenFeint Network Save Card can be thought of as simple flat file system that follows a user account around the network and restores application specific data to a game even if the account shows up on a different device. Defendant OpenFeint's the OFCloudStorage module allows you to store arbitrary game data on

1 OpenFeint servers. It is primarily intended for saving games. The module is represented by the  
2 include/OFCloudStorage.h header file. Each blob is distinguished by a key name unique within  
3 the context of the current application and user. The blob of data itself is passed through the API  
4 as an NSData object consisting of whatever binary data the application may store.

5 **2. Linking UDIDs to GPS Co-ordinates**

6 135. Plaintiffs and Class Members were not provided adequate notice, nor consented  
7 to, Defendant OpenFeint obtaining their “Fine” GPS co-ordinates, nor linking such to their  
8 mobile devices’ UDIDs. *Minor children’s* parents were not aware their *children’s* exact location  
9 was being accessed for tracking.  
10

11 136. Defendant OpenFeint obtained Plaintiffs’ and Class Members’ “Fine” GPS co-  
12 ordinates under false pretenses, by promoting its geo-location functionality as a means to play  
13 gamers “near you” or “near” the user’s location; thus user’s expected Defendant OpenFeint  
14 would obtain “coarse” co-ordinates that only provide a range within a city/ zip code. Although in  
15 actuality, Defendant OpenFeint used such as a ploy to obtain the user’s exact latitude and  
16 longitude for tracking purposes, and in order to link such to their mobile device’s UDIDs.  
17

18 137. While “Tom-Tom” like mapping applications do require “Fine” co-ordinates,  
19 obtaining the exact latitude and longitude within a few feet of the user, most applications such as  
20 weather applications, require only coarse co-ordinates. Defendant OpenFeint’s promotions were  
21 misleading:  
22

23 • “Geo-location Leaderboards. FINALLY! We had this feature 5 months ago before  
24 decide to switch to OF. Users love to know others play not far.”  
25  
26  
27  
28



Slava Bushtruk, iOS Dev Tips “Why Open Feint 2.4 rocks” Dec 25, 2009 (last accessed May 24, 2011), online: <http://iPhone-dev-tips.alterplay.com/2009/12/why-open-feint-24-rocks.html>

- Readme for OpenFeint iOS SDK 2.10.1
  - **Geolocation**
  - Allow **players** to **compete** with **players nearby**.
  - Distance based leaderboards.
  - Map view with player scores **near you**.

OpenFeint Developers Site, “Readme for OpenFeint iOS SDK 2.10.1” Last Updated: March 18, 2011 (last accessed May 24, 2011), online: <http://support.openfeint.com/dev/readme-for-openfeint-ios-sdk-2-10-1/>

138. *Minor children*, nor their parents, that provided Defendant OpenFeint with their co-ordinates to play fellow games in their region or city were aware that their exact latitude and longitude was being obtained and being used as a tracking device, causing serious privacy violations and security risks involving millions of *minor children*.

139. Permission to access location data is granted to the application by a popup displayed to the user. Defendant OpenFeint’s code running within the application may or may not then use this location information to send lat/long its servers. The app has its own code and the OpenFeint code is put inside the app code. Defendant OpenFeint’s server exists at its operation location; thus Defendant OpenFeint’s code is within the app code that sends the data it obtains to its server.

140. In this case, the user’s latitude and longitude is requested directly from the device’s GPS, through the developer API. No request is made “upstream” to the Mobile Device Operating System Manufacturer or carrier. Mobile device operating system manufacturers API’s

1 design prevents applications from doing this unless user consent has been given. The user's  
 2 latitude and longitude is fine-grained; risking a "leak" since it was able to be obtained through an  
 3 unauthenticated API call.

4 141. Both UDID and location data can be requested locally from the device. The  
 5 information is read from local hardware, so a request is made to the mobile device operating  
 6 system but not to mobile device operating system manufacturer's servers.

7 142. After the Cortesi Study, the unauthenticated part of Defendant OpenFeint's API  
 8 stopped returning unauthenticated latitude and longitude; thus evidencing Defendant  
 9 OpenFeint's knowledge that such permissions were not enabled by Plaintiffs and Class  
 10 Members, and of its ability to immediately cease such collection when notice of its act was  
 11 reported to them. However, Defendant OpenFeint *still* obtains latitude and longitude, *still* obtains  
 12 UDIDs, *still* aggregates data, and *still* links such to the user's UDIDs.

13 143. Defendant OpenFeint is a gaming platform that does not need GPS "Fine"  
 14 location linkage data, does not need to store it, nor create security risks by returning all of this  
 15 data unauthenticated through API calls that is obtained by a query on a user's UDIDs. OpenFeint  
 16 still aggregates UDIDs with GPS co-ordinates since it is still aggregating latitude/ longitude and  
 17 UDIDs. Portions of their API still returns user-associated GPS data, evidenced by passively  
 18 observing the traffic leaving and entering a phone during normal use. Such is a huge privacy risk,  
 19 exposing a user's information to any associated entity on the internet.

### 22 **3. Linking UDIDs to Facebook Profiles or Twitter**

23 144. Plaintiffs and Class Members were not provided adequate notice, nor consented  
 24 to, Defendant OpenFeint obtaining their Facebook or Twitter profiles, nor linking their mobile  
 25 device's UDIDs to their Facebook and/ or Twitter profiles. *Minor children's* parents were not  
 26 aware that their *children's* Facebook was being accessed for tracking.  
 27  
 28

1           145. Defendant OpenFeint obtained Plaintiffs' and Class Members' Facebook and/ or  
2           Twitter profiles under false pretenses by promoting its Facebook/ Twitter functionality as a  
3           means to associate with, and invite Facebook and/ or Twitter friends to play games. In actuality  
4           though, Defendant OpenFeint used such as a ploy to "scrape" the Plaintiffs' and Class Members'  
5           Facebook and/ or Twitter profile for Personally Identifiable Information, including but not  
6           limited to a user's pictures, in order to link such to their mobile device's UDIDs.

7           146. Defendant OpenFeint links UDIDs to Facebook accounts because users are still  
8           presented with the option to link their Facebook accounts to determine if their friends are playing  
9           the same Defendant OpenFeint affiliated gaming applications. Defendant OpenFeint then knows  
10          which accounts have which UDIDs, and which Facebook profiles are linked with which  
11          accounts, ergo, they can link Facebook profiles to UDIDs. Defendant OpenFeint only serves up  
12          an image through the Facebook Content Distribution Network (CDN). However, the CDN  
13          embeds the Facebook profile ID into the URL image thus giving the information needed to link  
14          back to a profile and a name.  
15

16          147. Plaintiffs and Class Members that enabled Defendant OpenFeint to link Facebook  
17          connect should have been provided adequate disclosure of what data would be transferred back  
18          and forth.  
19

20          148. Defendant OpenFeint obtained the Plaintiffs' and Class Members' pictures so as  
21          to link the identifier to the mobile device's owner's Facebook profile, which effectively puts a  
22          face behind that string of numbers and letters, thus creating a permanent, unalterable tracking  
23          cookie that can't be changed and is unknown to the user. Additional privacy and security  
24          concerns are increased because contained in the Facebook profile picture URL is the user's ID  
25          number for the social network which would then allow a third party to capture the user's name  
26          and other publicly shared information like their friend list and "likes" or connections.  
27  
28



1           149. While OpenFeint claims changes were made after the Cortesi study by reportedly  
2           ceasing obtaining Facebook picture profile, Defendant OpenFeint is *still* linking UDIDs to  
3           Facebook accounts.

4           **F. OpenFeint Controls All Facets of its OpenFeint Platform**

5           **1. OpenFeint Platform**

6           150. Since Defendant OpenFeint launched its mobile gaming platform business, it has  
7           maintained control of how mobile devices that have its OpenFeint platform work, how  
8           consumers use them, and what happens when consumers use them—including functions that  
9           Defendant OpenFeint controls, hidden from consumers' sight, although Defendant OpenFeint  
10          claims its practices would be transparent and inclusive.

11          151. Defendant OpenFeint controls the process for the development software as well—  
12          such as influencing developers to use Defendant OpenFeint's software development kit ("SDK"),  
13          and providing highly detailed guidelines for app development.

14          152. Defendant OpenFeint uses the mobile device operating systems, its Platform, and  
15          the software development process to completely control the user experience by constructing the  
16          user's entire mobile computing environment.

17          153. Behind Defendant OpenFeint's wall of control, it designs its App platform to be  
18          readily accessible to Application Developers, Ad networks and Web Analytic Vendors to access  
19          consumer's personal information. These companies not only provide an important revenue  
20          source for app developers who provide "free" apps through the Defendant OpenFeint Platform,  
21          but they also furnish the analytic data that demonstrates Defendant OpenFeint's market  
22          leadership which it so often herald in its quarterly investor conference calls. By helping finance  
23          third-party apps, these companies gain access to consumers' mobile devices to collect personal  
24          information they use to track and profile consumers, such as consumers' unique device  
25          information they use to track and profile consumers, such as consumers' unique device  
26          information they use to track and profile consumers, such as consumers' unique device  
27          information they use to track and profile consumers, such as consumers' unique device  
28          information they use to track and profile consumers, such as consumers' unique device

1 identifiers, geo-location histories, and Facebook profiles –highly personal details about who they  
2 are, who they know, and where they are.

3 154. Since Defendant OpenFeint launched its mobile device business, it has sought to  
4 completely control the user experience by controlling all facets of the mobile environment. It has  
5 differentiated itself in the marketplace by advertising that it provides its customers a tightly  
6 integrated user experience. With this control comes responsibility.

7  
8 **2. Defendant OpenFeint Controls Activities of Apps Within its Platform**

9 155. Plaintiffs and Class Members download apps that utilize a Mobile Device  
10 Operating System Manufacturer’s App Markets to Defendant OpenFeint’s Platform, but  
11 Defendant OpenFeint owns, controls, and operates its platform and activities of the downloaded  
12 apps within the OpenFeint Platform.

13 156. Numerous apps available from the App Markets are created by third-party  
14 developers. There are several hundred thousand third-party apps available at the App Markets.  
15 Some of these are ostensibly free and some are sold for a fee. OpenFeint distributes approved  
16 free apps through the OpenFeint Platform without charging the developer a fee. Defendant  
17 OpenFeint also distributes approved apps for which the consumer is charged a price set by the  
18 developer; Defendant OpenFeint collects the payment price through its revenue collection  
19 mechanism and retains a percent of the payment as its fee. Third-party apps include applications  
20 for business use, such as contact management and business expense tracking; personal finance  
21 use, such as trading; media, such as news outlets; education, such as childbirth education and  
22 children’s math learning; and entertainment, such as movie reviews and electronic games.

23  
24  
25 157. Defendant OpenFeint has control of the Application Developers by “vetting” the  
26 software applications for the devices, and controlling the OpenFeint Platform. No third party app  
27 developer is permitted to sell an app on the Defendant OpenFeint platform without entering into  
28

1 OpenFeint's Developer Agreement, nonetheless Defendant OpenFeint fails to control the  
2 developers by failing to implement a system to obligate the developers to abide by the terms of  
3 this agreement.

4 158. Defendant OpenFeint represents to every Defendant OpenFeint Platform user,  
5 through a required click-through agreement, assurances that the Defendant OpenFeint Platform  
6 will not permit apps that violate their privacy and security.

7 159. Defendant OpenFeint has also sought to exercise "indirect" control over what  
8 apps may use the Defendant OpenFeint platform. No developer is permitted to use the Defendant  
9 OpenFeint's platform without entering into OpenFeint's Developer Agreement. Defendant  
10 OpenFeint exercises its control of the OpenFeint Platform by implementing illusory contractual  
11 obligations in lieu of "vetting" the applications claiming to offer only apps that agree to its  
12 developer agreement; however users rely on Defendant OpenFeint to allow only those and found  
13 safe and appropriate.  
14

15 **3. Defendant OpenFeint Controls the Process for Apps Available on its**  
16 **Platform**  
17

18 160. In addition to controlling the characteristics and distribution of apps on its  
19 platform, Defendant OpenFeint exercises substantial control over its development and  
20 functionality.

21 161. Application Developers must also agree to the terms of Defendant OpenFeint's  
22 License Agreement. An app developed using Defendant OpenFeint's SDK will only function and  
23 interact within the Defendant OpenFeint platform and its features only in the ways permitted by  
24 the Defendant OpenFeint Agreement.  
25  
26  
27  
28

**G. Defendant OpenFeint is Negligent in Failing to Control OpenFeint Apps.**

**1. OpenFeint Has Failed To Use Its Control Over Defendant OpenFeint Apps, the Marketing of the Apps, the Programming of the Apps, its Platform to Protect User Privacy and the Security of User Data on its Platform**

162. Defendant OpenFeint's control of the user's experience includes restrictions, such as blocking consumers from modifying the Defendant OpenFeint platform. As a direct consequence of the control exercised by Defendant OpenFeint, Plaintiffs and the Class Members cannot reasonably review the privacy effects of apps and must rely on Defendant OpenFeint to fulfill its duty to do so. Defendant OpenFeint represents that it undertakes such a duty, that all apps available in its OpenFeint Platform have agreed to Defendant OpenFeint's mobile policies, and that it retains broad discretion to remove an app from the Defendant OpenFeint Platform.

163. A third party cannot upload an app for sale in the Defendant OpenFeint Platform until Defendant OpenFeint enters into a licensing agreement with the App developer; thereby giving its approval for sale of the app through the Defendant OpenFeint Platform. Defendant OpenFeint represents that an app may not access information from, or about, the user stored on the user's device unless the information is necessary for the advertised functioning of the app. Defendant OpenFeint represents that it does not allow one app to access data stored by another app. Defendant OpenFeint represents that it does not allow an app to transmit data from a user's mobile device to other parties without the user's consent. Defendant OpenFeint though does not review app source code, i.e. it does not review the code written by the developer in a programming language to inspect in order to determine if apps acquire users' personal information without the users' knowledge. Thus, Defendant OpenFeint's policy of not reviewing app's executable files permits apps that subject consumers to privacy exploits and security vulnerabilities to be offered in the Defendant OpenFeint Platform. Contrary to Defendant

1 OpenFeint's representations to consumers, Defendant OpenFeint does not analyze the traffic  
2 generated by apps to detect apps that violate the privacy terms of the Defendant OpenFeint  
3 Developer Agreement and Defendant OpenFeint's commitments to users.

4 164. Defendant OpenFeint recommends users install only applications they trust and  
5 provides assurances to users that their privacy and security shall be protected since suspicious  
6 apps can be uninstalled at any time, but Defendant OpenFeint fails to address how users can  
7 make informed decisions about which apps are trustworthy and which are not. However,  
8 knowing what an app is capable of is different than knowing what it actually does. There is no  
9 way of knowing what liberties the apps on competing platforms take with users' personal  
10 information, since Defendant OpenFeint failed to adequately inform users that their mobile  
11 device's UDIDs would be provided to any party.  
12

13 165. Defendant OpenFeint provides assurances within its terms of service and privacy  
14 policy that Plaintiffs and Class Members are not at risk for privacy violations and security risks,  
15 but fails to provide notice that the origin of mobile tracking by third parties originates with the  
16 third party's access to the user's UDIDs. Defendant OpenFeint's privacy policy fails to provide  
17 notice of the involvement of, and user data obtained by, advertising networks and web analytic  
18 vendors.  
19

20 166. Defendant OpenFeint fails to provide notice that mobile applications have access  
21 to a user's UDIDs which is passed to Defendant OpenFeint when it uses an application. Because  
22 the mobile device identifier is static and generally cannot be changed, Defendant OpenFeint  
23 falsely claims that a user's privacy is protected by associating your unique device identifier with  
24 an anonymous ID. In the online space, tracking is achieved through the placement of unique  
25 identification numbers on users' machines via the utilization of cookies. Mobile applications,  
26 however, run outside of the browser environment, hence the necessity to tie data to device IDs  
27  
28

1 instead. Because mobile applications run outside the web browser where Ad Networks and Web  
 2 Analytic Vendors access a user's web browser "cookies" for tracking; therefore a user can't  
 3 reliably apply their web browser preferences to block Ads within mobile applications.

4 167. Contrary to Defendant OpenFeint's representations, and without any permission  
 5 from its users, its platform design allows Application Developers to build apps that can easily  
 6 access the following Personally Identifiable Information on a consumer's mobile device:

7 • "International Mobile Subscriber Identity (IMSI), which remains unchanged even  
 8 when a user changes devices and which reveals the user's country and mobile operator;  
 9  
 10 • SIM card serial number (ICCID); and  
 11 • Universally unique device identifier (UUIDs), which OpenFeint refers to as  
 12 unique device identifiers (UDIDs), a number that uniquely identifies the particular Mobile  
 13 Device."

14 168. Nothing in the click-through agreement provided its users reasonable notice of the  
 15 mechanism and manner by which OpenFeint and its apps allow users to be tracked and have their  
 16 personal information shared by use of UDIDs. OpenFeint understands the significance of how  
 17 the unique device identifiers can violate a user's privacy, since UDID's information is  
 18 "Personally Identifiable Information" because, if combined with other information, such as other  
 19 information easily available on the mobile device, it can be used to personally identify a user.  
 20 Further, UDIDs are *globally* unique—no other device bears the same identifying numbers.

21  
 22 **2. Defendant Exploits the Access to Consumer Data by Creating Additional**  
 23 **Financial Incentives For Application Developers To Provide Additional Free and Paid**  
 24 **Apps to its Users Through App Markets.**

25  
 26 169. Notwithstanding Defendant OpenFeint's control of the user's experience, it  
 27 designs its Platform to be very open when it comes to disclosing information about consumers to  
 28

1 the Defendant, companies that incentivize Application Developers to provide the platform with  
2 free apps for mobile devices and provide Defendant OpenFeint the metrics to support its claims  
3 of market leadership. The personal and private information is of extreme interest to the  
4 Defendant Advertising Networks and Web Analytics companies. For this reason, the parties pay  
5 to support app development so that many apps are provided to consumers ostensibly “free” or at  
6 a lower cost.

7  
8 170. Defendant OpenFeint’s App Developer Agreement provides assurances to its  
9 users, including Plaintiffs and Class Members, that it shall provide protection and security for the  
10 privacy and legal rights of users.

11 171. Defendant OpenFeint provides assurances to Plaintiffs and Class Members that it  
12 shall provide protection and security for the privacy and legal rights of users and shall not allow  
13 activity that accesses their data in any unauthorized manner; however the Defendant OpenFeint  
14 provides no such protection.

15  
16 **3. Privacy Interests and Consent**

17 172. Plaintiffs and Class Members in this action consider the information from and  
18 about themselves on their mobile devices, their mobile device’s UDIDs personal data derived  
19 from Facebook and/ or Twitter profiles and GPS “Fine” co-ordinates to be personal and private  
20 information. Therefore, they do not expect their data to be collected, used by third parties, nor  
21 linked to their mobile device’s UDIDs without their express consent.

22 173. Plaintiffs and Class Members did not expect, receive notice of, nor consent to the  
23 Defendant tracking. Plaintiffs and Class Members did not expect, receive notice of, or consent to  
24 the Defendant’s acquisition of Plaintiffs’ and Class Members’ Personally Identifiable  
25 Information.  
26  
27  
28

1           174. The Defendant's activities were in conflict with its privacy policies and/or terms  
2 of use.

3           175. The Defendant's actions exceeded the scope of any authorization that was granted  
4 by Plaintiffs and Class Members at the time of enabling the OpenFeint Platform.

5           176. Plaintiffs and Class Members consider information about their mobile  
6 communications to be in the nature of confidential information, including their "Fine" geo-  
7 location, Facebook and/ or Twitter profiles, and do not expect it to be shared with an unaffiliated  
8 company. Defendant sells users' personal information after merging such with commercially  
9 available personal information obtained from a secondary information market which traffickers  
10 take substantial efforts to shield from the public. Defendant and other parties to the information  
11 market use the merger of personal information to effectively or actually de-anonymize  
12 consumers.  
13

14           177. Plaintiffs and Class Members did not consent to being personally identified to the  
15 Defendant or for their Personally Identifiable Information to be shared with and used on behalf  
16 of the Defendant.  
17

18           178. Defendant's actions were knowing, surreptitious, and without notice; therefore  
19 were conducted without authorization and exceeding authorization.

20           179. Defendant misappropriated Plaintiffs' and Class Members' personal information.

21           180. Consumers routinely engage in online economic exchanges with the websites they  
22 visit by exchanging their personal information for the websites' content and services, thereby  
23 reducing the costs consumers would otherwise have to pay. The transactions are value-for-value  
24 exchanges. This value-for-value exchange takes place particularly when an app is supported by  
25 advertising revenue, such as revenue the Defendant pays app developers.  
26  
27  
28



1           181. Because Defendant engaged in undisclosed collection of consumers' data and  
2 inadequately disclosed such, as alleged herein, those consumers did not receive the full value of  
3 their exchanges. In essence, Defendant raised the price consumers paid to use the app but instead  
4 of telling consumers or the website, Defendant simply reached around (or through) the website  
5 and into consumers' pockets, extracting their undisclosed premium in the form of consumers'  
6 information.

7           182. Because Defendant imposed an undisclosed cost on consumers by taking more  
8 information than they were entitled to take, Defendant's practices imposed economic costs on  
9 consumers.  
10

11           183. The scarcity of consumer information increases its value. Defendant devalued  
12 consumers' information by taking and propagating it.

13           184. The undisclosed privacy and information transfer consequences of Defendant's  
14 practices imposed costs on consumers in the form of the loss of the opportunity to have entered  
15 into value-for-value exchanges with other app providers whose business practices better  
16 conformed to consumers' expectations. Thus, Defendant's failure to adequately disclose the  
17 information practices and by using their lack of disclosure as a cover for taking consumers'  
18 information, Defendant imposed opportunity costs on consumers.  
19

20           185. Similarly, Defendant's lack of disclosure coupled with their taking of information  
21 imposed costs on consumers who would otherwise have exercised their rights to utilize the  
22 economic value of their information by declining to exchange it with Defendant or any other app  
23 provider.  
24

25           186. Consumers' information, an asset of economic value in the ways described above,  
26 has discernable value as an asset in the information marketplace where consumers may market  
27 their own information.  
28

187. Defendant's conduct alleged in this complaint constituted an ongoing course of conduct that harmed Plaintiffs and Class Members in general, and caused them to incur financial losses.

188. Defendant deprived Plaintiffs and Class Members of and/or diminished the economic value of their personal information.

189. Defendant used Plaintiffs' and Class Members' personal information for their own economic benefit.

190. Plaintiffs' and Class Members' experiences are typical of the experiences of Class Members.

191. The aggregated loss and damage sustained by the Class, as defined herein, includes economic loss with an aggregated value of at least \$5,000 during a one-year period.

192. Defendant perpetrated the acts and omissions set forth in this complaint through an organized campaign of deployment, which constituted a single act.

193. Plaintiffs and Class Members have been harmed by the Defendant's deceptive acquisition of their personal information, linkage of their mobile device's UDIDs, loss of their rights to use, share, and maintain the confidentiality of their information, each according to his or her own discretion.

#### **H. "Bandwidth Hog" – Economic Harm**

194. Defendant caused an economic harm to the Plaintiffs and Class Members that is actual, non-speculative, sum certain; and scientifically documented incurred by the unauthorized use of their mobile device's bandwidth; in that:

1. Plaintiffs and Class Members purchased a monthly limited bandwidth data plan for their mobile device from their carrier;
2. Plaintiffs and Class Members then downloaded Defendant

OpenFeint's affiliated applications and Defendant OpenFeint's API's integration directly to their mobile devices, "expecting" and agreeing to limited bandwidth consumption required and necessary to interact with the gaming applications and operate the mobile device.

3. However, Defendant OpenFeint and affiliated applications then made "calls" directing Plaintiffs' and Class Members' mobile device to third parties for marketing purposes, thereby depleting the purchased and linked bandwidth data plan of the Plaintiffs and Class Members, and such was *not* "expected" by the user, *not* required to interact with the gaming application, *not* agreed upon by the user, and *not* necessary to operate the mobile device.

195. Bandwidth is the amount of data that can be transmitted across a channel in a set amount of time. Any transmission of information on the internet includes bandwidth. Similar to utility companies, such as power or water, the "pipeline" is a substantial capital expenditure, and bandwidth usage controls the pricing model. Hosting providers charge users for bandwidth because their upstream provider charges them and so forth until it reaches the "back bone providers." Retail providers purchase it from wholesalers to sell to its consumers.

196. "Unlimited" plans are not unlimited. Major provider plans may refer to its plans as unlimited for marketing purposes, but the plans have limitations, usually noted in a footnote or link to another page discussing its limitations as to usage amounts. Providers could not possibly allow "unlimited" plans because servers do not have unlimited amounts of space. "Unlimited" data plans used to be unlimited until people started to figure out how to "tether," a method for connecting a computer to the internet via an internet-capable mobile phone. The term

1 “unlimited” is now used to define what is considered to be more than a reasonable amount of  
2 data allotment.

3 197. Network providers’ data plans charge consumers based upon such items as usage  
4 and “caps,” i.e. \$30.00 per month for an unlimited plan is standard; but limited plans have caps,  
5 such as: 256 GB per month. Some national providers charge \$1.00 per GB of bandwidth  
6 exceeding a certain cap. Whether the data plan is marketed as “unlimited” or “limited,” the costs  
7 for the plans are allocated based upon the bandwidth usage. Thus, as the standard use of  
8 bandwidth increases, so too does the plan costs. Since plans are based upon user’s average use,  
9 as consumer’s usage increases collectively, costs increase for all users, while individual  
10 bandwidth overages can be costly.

12 198. According to AT&T’s Web page detailing available data rate plans, users who  
13 pay \$60 for their DataConnect services get a monthly 5GB bandwidth cap and are to pay  
14 \$0.00048 per additional kilobyte of data they consume, or about \$500 per every gigabyte over  
15 the cap. Thus, a user who consumed three times the amount of data allowed by the company’s  
16 bandwidth cap would be charged about \$5,000 extra per month.”

18 Brad Reed, “User sues AT&T over \$5,000 Web bill” (last accessed April 15, 2011)  
19 online: <http://www.OpenFeint.com/legal/mobileme/en/terms.html>

20 199. The technology behind the World Wide Web is the Hypertext Transfer Protocol  
21 (HTTP) and it does not make any distinction as to the types of links, thus all links are  
22 functionally equal. Resources may be located on any server at any location. When a web site is  
23 visited, the browser first downloads the textual content in the form of an HTML document. The  
24 downloaded HTML document may call for other HTML files, images, scripts and/or style sheet  
25 files to be processed. These files may contain tags which supply the URLs that allow images to  
26 display on the page. The HTML code generally does not specify a server, meaning that the web  
27 browser should use the same server as the parent code. It also permits absolute URLs that refer to  
28

1 images hosted on other servers. Once the application has stored the data, it will attempt to send  
 2 information back to Application Developer affiliate's servers. In most cases this is done every  
 3 time you open and close an application. The data is continually tracked. An Application  
 4 Developer affiliate's enabled application does not take just one sample, it will record every use  
 5 of the application for the life of that application on your phone and your information is sent  
 6 automatically at a user's expense.

7           200. Ads consume vast amounts of bandwidth which results in slowing a user's  
 8 internet connection by using their bandwidth and diminishing the mobile devices battery life in  
 9 order to retrieve advertisements. Web Analytics devour more bandwidth than ads by accessing  
 10 bandwidth to download and run ad script, thus Plaintiffs and Class members that did not access  
 11 ads on an application still had the Defendant's Application Developers and Defendant  
 12 Application Affiliates use their bandwidth:

13           "When you're probing, you're using a users battery and data when they don't know about  
 14           it, but it's a faster way to build up data cause you're not waiting for the user to check in a  
 15           few times a day. You're pinging in 100 times a day...."

16           Yarrow, Jay "Everything You Need to Know About How Phones are Stalking You  
 17           Everywhere" (last accessed June 16, 2011) online:  
 18           <http://www.businessinsider.com/skyhook-ceo-2011-4#ixzz1PTSNO1pq>

19           201. Advertisers are now using the internet as their primary ad-delivery pipe,  
 20           continually upcoming and downloading data from its networks causing substantial bandwidth  
 21           use. Ads that were hidden in content, or bundled used substantial bandwidth, as did Application  
 22           updates. Web analytics activities delayed movement on a site, users on a site, using their  
 23           bandwidth, to complete its activities.

24           202. Application Developers and Application Developers Affiliates used ad content,  
 25           such as streaming video and audio, that required excessive Plaintiffs' and Class Members'  
 26

bandwidth, due in part, because there was no incentive to reduce the ad size used because it could directly pass costs for bandwidth and ad delivery content to Plaintiffs and Class Members, without the Plaintiffs and Class Members from having any notice, i.e. Plaintiffs and Class Members playing a game application, and at the same time, Application Developers and Application Affiliates were silently harvesting personal data and sending it to remote servers using Plaintiffs' and Class Members' bandwidth.

203. Defendant's use of the Plaintiffs' and Class Members' bandwidth for its data mining activities is similar in nature to a practice called "hot linking;" wherein one (1) server uses another server's bandwidth to send data. While it slows down the server, it also allows bandwidth costs to be transferred to another server. Defendant's data mining activities produces similar unauthorized bandwidth use. While only the tech savvy individuals are aware that their mobile devices are used as a server without their knowledge or consent, fewer individuals are aware of the extent that Application Developers and Application Developer Affiliates make "calls" to third parties, and of the amount of user's bandwidth used when a user merely accesses a site:

- "Let's look at what the popular twitterfon app does:
  - a. App start
  - b. Calls videoegg.adbureau.net, reports an Android is being used, sends UDID, app name & version.
  - c. Calls met.adwhirl.com, sends app ID, Android UDID, county
  - d. Calls twitter
  - e. Calls pagead2.OpenFeintsyndication.com
  - f. Calls beacon.pinchmedia.com, sends UDID, Android firmware, app ID & version, crack & jailbreak status, start & stop times
  - g. App close"

Yobie Benjamin, "iBigBrother? Android privacy issues may interest FCC and FTC" (last

accessed April 15, 2011) online: [http://www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?entry\\_id=46054](http://www.sfgate.com/cgi-bin/blogs/ybenjamin/detail?entry_id=46054)

204. Excluding the amount of bandwidth that the Plaintiffs and Class members use, the amount necessary to operate their mobile device, and the expected amount by the user's interaction with the gaming application, and that of which was agreed upon by the user, Defendant's unauthorized data mining activities caused substantial bandwidth use to the Plaintiffs and Class Members that resulted in actual out of pocket expenditures. Defendant's activities which include, but are not limited to, the following:

- a) Transmittal of and access to Plaintiffs and Class Members UDIDs;
- b) Loading of ads first before content, bundling ads, and ads with excessive bandwidth;
- c) Use of SDKs, and its functions within Plaintiffs' and Class Members' mobile device;
- d) Harvesting of Plaintiffs' and Class Members' mobile device data;
- e) Harvesting of Plaintiffs and Class Members' Personally Identifiable Information;
- f) "Background" activities including "data mining;"
- g) "Push notifications" of content to user's mobile device; and
- h) Re-direction of Plaintiffs' and Class Members' mobile devices to make "calls" to Defendant OpenFeint and affiliated applications for marketing purposes.

205. The amount of bandwidth use on mobile devices can be measured directly by analyzing the logged traffic use which varies generally between 0 bytes and about 500k per session. The traffic use, whether expected by the user or not, is part of the normal operation of the device. Application traffic analysis shows the majority of the traffic is OpenFeint's

1 integration, including the Facebook traffic (fbcdn), the Twitter image traffic, and the direct  
2 traffic to OpenFeint's servers. The traffic to third parties for marketing purposes, such as the  
3 Application Developer's re-direction to third party domains is not required, nor authorized by the  
4 user; moreover the user is never prompted to allow it or notified that it has occurred.

5       206. The basic nature of HTTP is a challenge-response protocol. For each request,  
6 there is necessarily a response. Conventional technical usage would refer to the challenge-  
7 response pair as a single "call."  
8

9       207. Defendant OpenFeint's Platform allows for the use of newsletters and updates to  
10 allow the continuous interaction with the user's device; however such uses substantial  
11 bandwidth. Defendant OpenFeint and gaming applications want to have content sent  
12 continuously from the games to the users since the games are rated by usage and do not  
13 differentiate between players' usage as opposed to "push notification content," and all in an  
14 effort to move up to top spots on the app lists for most visited applications which increase sales.  
15 The content push and calls repeat periodically, and use a substantial amount of Plaintiffs' and  
16 Class Members' bandwidth. This type of user traffic is usually triggered on use - i.e. traffic  
17 would be sent every time the app is started up, or whenever some other trigger event occurred  
18 during use.  
19

20       208. Plaintiffs and Class Members that accessed Defendant OpenFeint's applications  
21 were re-directed to multiple domains, without their knowledge or consent; thus Plaintiffs' and  
22 Class Members' bandwidth was used for Defendant OpenFeint's and OpenFeint affiliated  
23 applications' marketing activities. The "Cortesi Study" was updated recently and revealed that  
24 84% of the apps tested contacted one or more domains during use. At the extreme end, iDestroy,  
25 a Defendant OpenFeint affiliated application, contacted fourteen (14) domains, including the  
26 following three (3) different ad networks and Defendant OpenFeint *after* the user accessed the  
27  
28



application:

- 1) idestroyhttp://mob.adwhirl.com
- 2) http://analytics.localytics.com
- 3) https://p18-buy.itunes.apple.com
- 4) https://api.openfeint.com
- 5) http://ax.init.itunes.apple.com
- 6) http://mmv.admob.com
- 7) https://idcodes.appspot.com
- 8) http://met.adwhirl.com
- 9) http://www.idestroyapp.com
- 10) http://r.admob.com
- 11) http://mm.admob.com
- 12) http://a.admob.com
- 13) http://itunes.apple.com
- 14) https://ws.tapjoyads.com

Aldo Cortesi, "How UDIDs are used: a survey," May 19, 2011 (last accessed May 20, 2011), online: <http://corte.si/posts/security/apple-udid-survey/index.html>

209. Defendant OpenFeint's servers must interface with, and draw bandwidth from, Plaintiffs' and Class Members' mobile device's limited bandwidth data plan in order to complete its tracking practices. Like a "bad" neighbor that sneaks over in the dead of night to plug in an extension cord into their neighbor's electrical outlet to "suck out" kilowatts, Defendant OpenFeint was "hogging" the Plaintiffs' and Class Members' purchased and limited bandwidth plan, and not reimbursing Plaintiffs and Class Members for using their limited data plan. The economic harm is actual, non-speculative, out of pocket, sum certain; and scientifically documented:

- "If consumers perceive that rich media ads and other marketing activities affect their consumption of bandwidth, and that they are paying to watch ads, it could have affect mobile advertising."

Chantal Tode, "T-Mobile's new pricing reflects concern over growing bandwidth use" (last accessed May 28, 2011) online: <http://mobilemarketer.com/cms/news/carrier-networks/10015.html>

### **I. Defendant's Harmful Business Practices**

210. Defendant's business practice unfairly wrests control from Plaintiffs and Class

1 Members who choose to block and delete any mobile tracking device on their mobile devices in  
2 order to avoid being tracked. Plaintiffs and Class Members who are aware of being tracked may  
3 attempt to delete any and all tracking devices periodically, believing that the new applications  
4 they receive will not contain new unique identifiers; thus hindering the ability of advertising  
5 networks to track their behavior across sites. However, such shall be using a false theory. Using  
6 databases overrides this attempt, with little available redress for users.

7  
8 211. Defendant failed to disclose that its applied technologies, such as tracking UDIDs,  
9 provide Defendant with the ability to surreptitiously intercept, access, and collect electronic  
10 communications and information from unsuspecting Plaintiffs and the Class Members, thereby  
11 obtaining personal and private information, monitoring their internet activity, and creating  
12 detailed personal profiles based on such information.

13 212. Defendant intercepted Class Members' electronic communications for the purpose  
14 of committing a tortious or criminal act, and violated the constitutional rights of Plaintiffs and  
15 Class Members.

16  
17 213. In all cases where some notice was provided, that notice was insufficient,  
18 misleading, and inadequate. Consent under such circumstances was impossible.

19 214. Defendant failed to provide opt-out functionality for Plaintiffs and Class  
20 Members, so that Plaintiffs and Class Members could set their security preferences.

21 215. Defendant failed to implement a software program that would scramble the  
22 UDIDs, creating a unique ID for each application.

23  
24 216. In any case where the opportunity of "opting out" of the Defendant service was  
25 provided, such "opt-out" rights were misleading, untrue, and deceptive.

26 217. In no case was the collection of all Internet communication data between the  
27 consumer and the Internet halted or affected in any way. All data was still collected. Thus, the  
28

1 provision of the opportunity for opting-out was, itself, totally misleading.

2       218. Plaintiffs and the Class Members did not voluntarily disclose their personal and  
3 private information to the Defendant's tracking, let alone their mobile device habits to Defendant  
4 - and indeed never even knew that Application Developers Affiliates existed or conducted data  
5 collection and monitoring activities upon and across its Plaintiffs' and Class Members'  
6 applications. Plaintiffs and the Class Members provided such information, and had specific  
7 mobile device habits monitored, without their knowledge or consent, and would not have  
8 consented having their personal and private information, including use of their on-line Facebook  
9 and/ or Twitter profiles, or "Fine" geo-location used for Defendant's commercial gain.  
10

11       219. Defendant did not obtain consent from Plaintiffs and Class Members for any  
12 collection or use of any and all data derived in whole or part from use of UDIDs. Plaintiffs and  
13 Class Members were not allowed to decline consent at the time such statement was presented.  
14

15       220. Defendant did not obtain consent from Plaintiffs and Class Members for any  
16 disclosure of covered information to unaffiliated parties. Plaintiffs and Class Members were not  
17 allowed to decline consent at the time such statement was presented.

18       221. Defendant intentionally accessed data, derived in whole part, from Plaintiffs' and  
19 Class Members' mobile devices without authorization or exceeded authorized access to obtain  
20 information from a protected mobile device through interstate communications.

21       222. Defendant sold, shared, and/or otherwise disclosed covered information of Class  
22 Members to an unaffiliated party without first obtaining the consent of the Class Members to  
23 whom the covered information belonged.  
24

25       223. At all relevant times, Plaintiffs' and Class Members' personal and private  
26 information was electronically intercepted and/or accessed by and transmitted to Defendant on a  
27 regular basis, without alerting Plaintiffs and Class Members in any manner. As a result,  
28

1 Defendant was able to and did obtain data derived in whole or part from Plaintiffs' and Class  
2 Members' mobile devices and/or intercept their electronic communications without  
3 authorization. Defendant has obtained, compiled, and used this personal information for its own  
4 commercial purposes.

5 224. Defendant intercepted Plaintiffs' and Class Members' electronic communications  
6 for the purposes of obtaining mobile device data, using UDIDs from Plaintiffs' and Class  
7 Members' mobile devices by repeatedly accessing electronic communications without Plaintiffs'  
8 and Class Members' knowledge and consent to profile, secretly track Plaintiffs' and Class  
9 Members' activities on the Internet and collect personal information about consumers; and profit  
10 from the use of the illegally obtained information, all to Defendant's benefit and Plaintiffs' and  
11 Class Members' detriment.

12 225. Defendant intentionally intercepted, endeavored to intercept, or procured another  
13 entity to intercept or endeavor to intercept the electronic communication of Plaintiffs and Class  
14 Members.

15 226. Defendant has, either directly or by aiding, abetting and/or conspiring to do so,  
16 knowingly, recklessly, or negligently disclosed, exploited, misappropriated and/or engaged in  
17 widespread commercial usage of Plaintiffs' and the Class Members' mobile device data,  
18 obtained private and sensitive information for Defendant's own benefit from unauthorized use of  
19 their UDIDs, without Plaintiffs' or the Class Members' knowledge, authorization, or consent.  
20 Such conduct constitutes a highly offensive and dangerous invasion of Plaintiffs' and the Class  
21 Members' privacy.

22 227. Defendant used and consumed the resources of the Plaintiffs' and Class  
23 Members' mobile devices by gathering user information, adding such information to their mobile  
24 database, and transferring such to Defendant.

228. Defendant caused harm and damages to Plaintiffs' and Class Members' mobile devices finite resources, depleted and exhausted its memory, thus causing an actual inability to use it for its intended purposes. Defendant caused significant unwanted CPU activity, usage, and network traffic, resulting in instability issues.

229. Defendant caused harm and damages to the Plaintiffs and Class Members including, but not limited to, consumption of their device's finite resources, memory depletion, and bandwidth, which resulted in the actual inability to use if for its intended purposes.

230. Defendant's activity was not evident. Plaintiffs and Class Members assumed that the issues related to hardware, Windows installation problems, or viruses, and resorted to contacting technical support experts, or even buying a new mobile device because the existing system mobile device posed privacy risks.

231. Defendant harmed Plaintiffs and Class Members by its actions which included, but not limited to, the following:

- a) Loss of valuable data by attempts to remove UDIDs and databases once discovered;
- b) Incurred economic losses accompanied by an interruption in service;
- c) Functionality of mobile device was interfered with, including an inability of applications visited once content was disabled;
- d) Information was deleted, otherwise made unavailable;
- e) Impaired the integrity and availability of data, programs, and information;
- f) Mobile device bandwidth; and
- g) Inability to resell the user's mobile device with UDIDs associated with user's aggregate mobile device data.

232. Defendant impacted the Plaintiffs' and Class Members' ability to sell their mobile devices since the mobile device's UDIDs will have aggregated data linked to such device and will continue to provide aggregated cross platform data. The new mobile device owner will then

1 be provided tracking advertisements related to the past mobile device owner.

2 233. Plaintiffs and Class Members were personally injured, as that term is recognized  
3 within the cyber and technology industry, when Defendant intentionally, or in the alternative,  
4 negligently, obtained, processed, and disseminated content, obtained without authorization,  
5 invaded Plaintiffs' and Class Members' right of privacy, which portrayed Plaintiffs and Class  
6 Members in a false light by publicly disclosing private facts through their intrusion into the  
7 Plaintiffs' and Class Members' personal mobile browsing activity.

8 234. Defendant's impact upon the Plaintiffs' and Class Members' mobile devices was  
9 significant resulting in a substantial reduction in available memory, processing power and  
10 database storage.

11 235. Defendant's interaction with the Plaintiffs' and Class Members' mobile device  
12 was not temporarily, but a permanent use of the mobile devices' storage resulting in a significant  
13 loss of use and potentially overwhelming the Plaintiffs' and Class Members' databases.

14 236. Plaintiffs and Class Members expended money, time, and resources investigating  
15 and attempting to mitigate their mobile devices diminished performance, in addition to  
16 investigating and attempting to remove the Defendant's tracking mechanisms.

17 237. Plaintiffs and Class Members conducted a damage assessment once they became  
18 aware of Defendant's practices, made the basis of this action, to attempt to restore any affected  
19 data, program, system or information.

20 238. Defendant's conduct caused outrage, mental suffering, harm, and humiliation to  
21 Plaintiffs' and Class Members' privacy expectations.

22 239. Defendant intentionally disposed of the Plaintiffs' and Class Members' property  
23 by using and intermeddling with their mobile devices so as to impair its condition, quality, and  
24 value, thus preventing the Plaintiffs and Class Members from using their mobile devices for a  
25

1 substantial time.

2           240. Defendant's Unique Device Identifier remains identified with the Plaintiffs' and  
3 Class Members' devices, thus the value of the device has been diminished, or now has no value  
4 for resale.

5           241. Defendant's activities occurred throughout the United States. Defendant secretly  
6 obtained personal and private information from Plaintiffs and the Class Members - a course of  
7 action and a body of information that is protected from interception, access, and disclosure by  
8 federal law.

9  
10           242. Defendant used, interfered with, and intermeddled with Class Members'  
11 ownership of their personal property, namely, their mobile devices, by directly or indirectly:  
12 secretly obtaining Plaintiffs' and Class Members' data derived from their UDIDs; secretly  
13 accessing their mobile devices to obtain information contained in and enabled by the Unique  
14 Device Identifier; and secretly collecting personal data and information regarding each Plaintiffs'  
15 and Class Members' Internet surfing habits contained in electronic storage on his/her mobile  
16 device.

17  
18           243. Defendant failed to disclose that UDIDs are used to track and store information  
19 regarding consumers' Internet use and other forms of advertisements on consumers' mobile  
20 devices based on such use. The installation of such tracking device would be material to  
21 consumers in their decision whether to install the software offered by Defendant.

22           244. Defendant's technology wrongfully monitored Internet users' activities at each  
23 and every affiliated application visited. The wrongfulness of this conduct is multiplied by the  
24 fact that Defendant aggregates this information about users' habits across numerous applications  
25 and unjustly enriched Defendant to the severe detriment of Plaintiffs and the Class Members.  
26 Plaintiffs and the Class Members have been harmed, as they have been subjected to repeated and  
27  
28

1 unauthorized invasions of their privacy - violations which continue to this day.

2 245. Without remedy, Plaintiffs and Class Members will continue to be tracked by  
3 dozens of companies — companies they've never heard of, companies they have no relationship  
4 with, companies they would never choose to trust with their most private thoughts and reading  
5 habits.

6 246. Defendant's privacy documents, which include, but are not limited to, its privacy  
7 policy and terms of use, intentionally, or in the alternative, negligently, omit notice of any and all  
8 of its activities made the basis of this action. Such omissions relate in whole or part, to  
9 Defendant's intentional, or in the alternative, negligent, omission within its privacy documents to  
10 any and all activities related to the basis of this action and notice of its activities with each  
11 Affiliate.  
12

13 247. Defendant's privacy documents fail to provide adequate notice that third parties,  
14 made the basis of this action, would be allowed access to personal behavioral data of their users,  
15 including but not limited to, such data embedded with their applications, which in turn shares the  
16 data with its marketing partners or corporate affiliates and subsidiaries. Therefore, user behavior  
17 will be profiled by any other entities with whom those sites may choose to share this  
18 information. While Defendant's privacy documents state they do not share data with third  
19 parties, they do share data with affiliates, suggesting that they only share data with companies  
20 under the same corporate ownership.  
21

22 248. Defendant's privacy documents referenced the use of analytics, but state such is  
23 used only for audience measurement and not behavioral ad-targeting.  
24

25 249. Defendant's privacy documents do not expressly state that if a user does not  
26 enable Defendant's platform to be downloaded that behavioral information will not be collected  
27 pertaining to the user.  
28



1           250. Defendant's privacy documents falsely imply some level of protection for the  
2 user. Defendant's privacy documents are sufficiently vague so as to refrain from fully disclosing  
3 information to their users about the information collected through their applications, their  
4 associated entities, how the information is used, and the purposes for the collection and use of  
5 this information. Thus, negating the possibility for their users to provide informed and  
6 meaningful consent to these practices. Without adequate notice and informed and meaningful  
7 user consent, users had no control over their personal information. The potential privacy dangers  
8 were not readily apparent to most users.  
9

10           251. Defendant's privacy documents require college-level reading skills for  
11 comprehension and include substantial legalese, ambiguous and obfuscated language designed to  
12 confuse, disenfranchise, and mislead the users.

13           252. Defendant's privacy documents incorporate a multitude of hedging and modality  
14 markers so as to minimize their use of covert surveillance technology and data-gathering tools.  
15 Defendant sends mixed messages related to privacy controls by advising users that choosing to  
16 exercise such controls would cause in whole, or part, diminished functionality of their  
17 applications.  
18

19           253. Defendant's privacy documents describe "associations," misleading the users to  
20 interpret them to be associated corporate subsidiaries while withholding accurate information  
21 that such includes other entities than advertising networks, such as: advertising networks, data  
22 exchanges, traffic measurement service providers, marketing and analytic service providers.  
23

24           254. Defendant's applications and its tracking services are owned by parent companies  
25 that have many subsidiaries. Defendant fails to provide adequate information about third-party  
26 information sharing, different than affiliate sharing, which is subject to more restrictions,  
27 including opt-in or opt-out consent requirements. These restrictions are based upon the  
28

1 heightened risk associated with sharing information with unrelated entities because of the  
2 difference in incentives between them and the original entity that collected the user data.

3 255. Defendant does not make adequate distinctions between sharing with affiliates,  
4 contractors, and third parties. Instead, Defendant vaguely states that they do not share user data  
5 with unrelated third parties and vaguely discloses that they share data with affiliates. Users must  
6 interpret an affiliate to be a third party, but given the actual usage of these terms of Affiliates'  
7 privacy policies, that assumption would be mistaken.

8 256. Defendant does not identify the corporate families to which its applications  
9 belong, since they provide no privacy documents. This makes it difficult for a user to discover  
10 exactly who such associated entities are, thus making their practices deceptive. A practice is  
11 deceptive if it involves a representation, omission or practice that is likely to mislead a consumer  
12 acting reasonably in the circumstances, to the consumer's detriment. The conflicting statements  
13 in the privacy policies would most likely confuse or mislead a reasonable consumer. The  
14 confusion would also likely be to their detriment, as surveys indicate that users do not want  
15 companies to collect data about them without permission.

16 257. Defendant's privacy documents discuss that the data collection practices of  
17 entities associated with their corporations are outside the coverage of their privacy policies. This  
18 appears to be an attempt to create a critical loophole compounding their attempts to violate the  
19 privacy protection of their users.

20 258. Defendant's privacy documents fail to adhere to an adequate notice and choice  
21 regime, predicated on user choice, and informed by privacy policies. Defendant's privacy  
22 documents provided nuanced situations that created conditional yes or no answers to these basic  
23 questions about a site's data collection and sharing practices, thus it is unclear how an average  
24 user could ever understand these practices since the nuances were not explained in the privacy  
25  
26  
27  
28

1 policy. Choice, therefore, could not be inferred.

2 259. Defendant's privacy documents carefully attempt to parse the definitions of  
3 phrases related to their tracking activity. Their privacy documents are more nuanced than such  
4 categorized analysis allows for by means of embedding any and all purposes for its use of:  
5 surveillance technology into the user's mobile device hardware; user's mobile device hardware  
6 to store data; technology to allow the perpetual mobile device tracking and surveillance of any  
7 and all mobile device Internet activity of the Defendant OpenFeint users. It is evidenced by the  
8 attempt of Defendant OpenFeint to hide its covert activity by referring to their use of "other  
9 technologies," or "similar technologies," and omitting information that UDIDs would be used to  
10 track users, and its perpetual existence on a user's mobile device.  
11

12 260. Defendant's privacy documents fail to provide notice that their data storage  
13 practices as they relate to the period for which user data is stored, have no term period, and are  
14 indefinite.  
15

16 261. Defendant's privacy documents' verbiage was deceptive by design. This  
17 deception is especially troubling when compared with the obligation imposed upon their mobile  
18 device visitors to download, read, and comprehend the vast amount of documents required to  
19 protect one's mobile device privacy, complicated by the cumulative effect of such task.  
20

21 262. In addition to downloading, reading and comprehending all of Defendant  
22 OpenFeint's and Application Developers privacy documents, although most did not provide  
23 such, its users would be required to locate and attempt to do the same for Application Developers  
24 Affiliates. To accentuate the improbability of completing this task, Plaintiffs and Class Members  
25 were not provided information of the identity of Application Developer's Affiliates, nor its  
26 association with Defendant OpenFeint.

27 263. Application Developer Affiliates' privacy documents reveal omissions related in  
28

1 whole or part, intentionally, or in the alternative negligently, to any and all activities related to  
2 the basis of this action and notice of its activities with Application Developers.

3 264. Defendant's mobile device privacy protection was premised upon imposed  
4 requirement to download, read, and comprehend the accumulation of all privacy documents of  
5 all involved entities.

6 265. A millisecond was the time allotted to the Plaintiffs and Class Members download  
7 of a Defendant OpenFeint Market affiliated application, before Defendant OpenFeint,  
8 Application Developers and Application Developer Affiliates intentionally, and without user's  
9 authorization and consent, had Defendant OpenFeint transmit, and/or allowed access to, data  
10 related to whole or part, from the Plaintiffs' and Class Members' mobile devices' UDIDs. Such  
11 occurred without the benefit of being advised of the association between Defendant OpenFeint,  
12 Application Developer and its Application Developer Affiliate, or provided adequate time to  
13 access, read, and comprehend the Terms of Service/Use and Privacy Policy for all parties which  
14 had privacy policies. While only the most technical savvy mobile device users were familiar with  
15 UDIDs, a finite amount of individuals even knew about "UDIDs," let alone could possibly  
16 comprehend the technical aspects inherent within the Defendant's privacy documents.

17 266. The collection, use and disclosure of tracking data, such as obtaining a users'  
18 UDIDs by Defendant to provide its services, implicates Plaintiffs' and Class Members' privacy  
19 and physical safety. Such information is afforded special attention due to the consequences for  
20 both privacy and physical safety that may flow from its disclosure. The heightened privacy and  
21 physical safety concerns generated by the collection, use and disclosure of location information  
22 are apparent in U.S. law that creates restrictive consent standards for its use and disclosure in the  
23 private sector in the context of telecommunications services.

24 267. Defendant OpenFeint's platform to aggregate user data, in association with its  
25  
26  
27  
28

1 user's UDIDs has the potential to transform the World Wide Web from a largely anonymous  
2 environment into one where individuals are expected, or even required, to identify themselves in  
3 order to participate in online activities, communicate, and make purchases. This occurrence  
4 would represent a grave erosion of consumer's online privacy. Many of the activities in which  
5 individuals engage on the Web do not require the collection of identifiers or personal information  
6 of any type. "Free" applications involve a user not paying for a product, but paying with their  
7 personal information, which becomes the actual product.  
8

9 268. The tracking and monitoring of mobile device usage will have a negative effect  
10 on individuals' access to information. The anonymity that the Internet affords individuals has  
11 made it an incredible resource for those seeking out information. Particularly where the  
12 information sought is on controversial topics such as sex, sexuality, or health issues such as HIV,  
13 depression, and abortion; the ability to access information without risking identification has been  
14 critical. It will result in increased pressure on individuals to permit the collection of the UDIDs,  
15 and other information that can be tied to it, as a quid pro quo of engaging in transactions and  
16 interactions online, thereby placing a burden on individuals who choose to protect their privacy.  
17

18 269. Because of Defendant OpenFeint's market dominance, UDIDs have the potential  
19 to become the unique identifier for nearly everyone on the Internet – fundamentally changing the  
20 mobile internet experience from one where consumers can browse and seek out information  
21 anonymously, to one where an individual's every move is recorded. Our society's experience  
22 with unique identifiers suggests that accessing UDIDs from mobile devices to link Personally  
23 Identifiable Information with shall erode individual privacy. The history of the Social Security  
24 Number reveals the unrelenting pressures to expand the use of an identifier once it is created --  
25 even where its use is initially curtailed by federal policy. Once a unique device identifier is  
26 capable of identifying and tracking individuals in the online environment is created, it will be far  
27  
28

more difficult to limit its use. The Social Security Number (SSN) offers a compelling example of how a unique identifier can undermine individual privacy and become a de facto national identifier. The UDID has the potential though to further the surreptitious collection and use of data without an individual's consent. Unlike a real world identifier, such as the Social Security Number, the UDID, a virtual identifier, is capable of being collected and used without the individual's knowledge and consent causing privacy and security violations.

### **CLASS ALLEGATIONS** **Allegations as to Class Certification**

270. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiffs bring this action as a Class action, on behalf of themselves and all others similarly situated as members of the following Classes (collectively, the "Class"):

- a) U.S. Resident Class: All persons residing in the United States that downloaded and enabled a mobile application affiliated with OpenFeint, from February 17, 2009 to the date of the filing of this complaint.
- b) Injunctive Class: All persons after the date of the filing of this complaint, residing in the United States that downloaded and enabled a mobile application affiliated with OpenFeint after the date of the filing of this complaint.

271. The Class action period, (the "Class Period"), pertains to the dates, February 17, 2009 to the date of Class certification.

272. Plaintiffs reserve the right to revise the definitions of the Classes based on facts learned in the course of litigation of this matter.

273. On behalf of the U.S. Resident Class, Plaintiffs seek equitable relief, damages and injunctive relief pursuant to:

- a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- b) Electronic Communications Privacy Act, 18 U.S.C. § 2510;
- c) California's Computer Crime Law, Penal Code § 502;

- d) California's Invasion of Privacy Act, Penal Code § 630;
- e) Consumer Legal Remedies Act, ("CLRA") California Civil Code § 1750;
- f) Unfair Competition, California Business and Professions Code § 17200;
- g) Breach of Contract;
- h) Breach of Implied Covenant of Good Faith and Fair Dealing;
- i) Conversion;
- j) Negligence; and
- k) Trespass to Personal Property / Chattels

274. On behalf of the Injunctive Class, Plaintiffs seek only injunctive relief.

275. **Persons Excluded From Classes:** Subject to additional information obtained through further investigation and discovery, the foregoing definition of the Class may be expanded or narrowed by amendment or amended complaint. Specifically excluded from the proposed Class are Defendant, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint ventures, or entities controlled by Defendant, and their heirs, successors, assigns, or other persons or entities related to or affiliated with Defendant and/or their officers and/or directors, or any of them; the Judge assigned to this action, and any member of the Judge's immediate family.

276. **Numerosity:** The members of the Class are so numerous that their individual joinder is impracticable. Plaintiffs are informed and believe, and on that basis allege, that the proposed Class contains tens of thousands of members. The precise number of Class Members is unknown to Plaintiffs. The true number of Class Members is known by Defendant, however and, thus, Class Members may be notified of the pendency of this action by first Class mail, electronic mail, and by published notice. Upon information and belief, Class Members can be identified by the electronic records of Defendant.

277. **Class Commonality:** Pursuant to Federal Rules of Civil Procedure, Rule 23(a)(2)

1 and Rule 23(b)(3), are satisfied because there are questions of law and fact common to Plaintiffs  
 2 and the Class, which common questions predominate over any individual questions affecting  
 3 only individual members, the common questions of law and factual questions include, but are not  
 4 limited to:

- 5 a) What was the extent of Defendant's business practice of transmitting,  
 6 accessing, collecting, monitoring, and remotely storing users' Unique Device  
 7 Identifiers ("UDIDs") obtaining a user's Personally Identifiable Information,  
 8 and linking the aggregated data with the user's UDIDs and how did it work?
- 9 b) What information did Defendant's collect from its business practices of  
 10 transmitting, accessing, collecting, monitoring, and remotely storing users'  
 11 Unique Device Identifiers ("UDIDs"), and what did it do with that  
 12 information?
- 13 c) Whether users, by virtue of their downloading the application, had pre-  
 14 consented to the operation of Defendant's business practices of transmitting,  
 15 accessing, collecting, monitoring, and remotely storing users' Unique Device  
 16 Identifiers ("UDIDs");
- 17 d) Was there adequate notice, or *any* notice, of the operation of Defendant's  
 18 business practices of transmitting, accessing, collecting, monitoring, and  
 19 remotely storing users' Unique Device Identifiers ("UDIDs") provided to  
 20 Plaintiffs and Class Members?
- 21 e) Was there reasonable opportunity to decline the operation of Defendant's  
 22 business practices of transmitting, accessing, collecting, monitoring, and  
 23 remotely storing users' Unique Device Identifiers ("UDIDs") provided to  
 24 Plaintiffs and Class Members?
- 25 f) Did Defendant's business practices of obtaining, collecting, monitoring, and  
 26 remotely storing users' Unique Device Identifiers ("UDIDs") disclose,  
 27 intercept, and transmit Personally Identifying Information, or Sensitive  
 28 Identifying Information, or Personal Information?
- g) Whether Defendant devised and deployed a scheme or artifice to defraud or  
 conceal from Plaintiffs and the Class Members Defendant's ability to, and  
 practice of, intercepting, accessing, and manipulating, for its own benefit,  
 Personal Information, and tracking data from Plaintiffs' and the Class  
 Members' personal mobile device via the ability to track their mobile device  
 by tracking its UDID on their mobile device;
- h) Whether Defendant engaged in deceptive acts and practices in, connection  
 with its undisclosed and systemic practice of transmitting, accessing and/or  
 disclosing unique identifiers, tracking data, and Personal Information on  
 Plaintiffs' and the Class Members' personal mobile device and using that data



1 to track and profile Plaintiffs' and the Class Members' Internet activities and  
 2 personal habits, proclivities, tendencies, and preferences for Defendant's use  
 and benefit;

- 3 i) Did the implementation of Defendant's business practices of transmitting,  
 4 accessing, collecting, monitoring, and remotely storing users' Unique Device  
 Identifiers ("UDIDs") violate the Computer Fraud and Abuse Act, 18 U.S.C.  
 5 §§ 1030?
- 6 j) Did the implementation of Defendant's business practices of transmitting,  
 7 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") violate the Electronic Communications Privacy Act, 18  
 8 U.S.C. § 2510?
- 9 k) Did the implementation of Defendant's business practices of transmitting,  
 10 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") violate the Violations of California's Computer Crime  
 11 Law, Penal Code § 502?
- 12 l) Did the implementation of Defendant's business practices of transmitting,  
 13 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") violate the Violations of the California Invasion of  
 Privacy Act, Penal Code § 630?
- 14 m) Did the implementation of Defendant's business practices of transmitting,  
 15 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") violate the Violations of the Consumer Legal Remedies  
 16 Act, ("CLRA") California Civil Code § 1750?
- 17 n) Did the implementation of Defendant's business practices of transmitting,  
 18 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") violate the Violation of Unfair Competition, California  
 19 Business and Professions Code § 17200?
- 20 o) Did the implementation of Defendant's business practices of transmitting,  
 21 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") involve a Breach of Contract?
- 22 p) Did the implementation of Defendant's business practices of transmitting,  
 23 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") involve a Breach of Implied Covenant of Good Faith  
 24 and Fair Dealing?
- 25 q) Did the implementation of Defendant's business practices of transmitting,  
 26 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") involve a Conversion?
- 27 r) Did the implementation of Defendant's business practices of transmitting,  
 28 accessing, collecting, monitoring, remotely storing users' Unique Device  
 Identifiers ("UDIDs") involve a Negligence.

- s) Did the implementation of Defendant's business practices of transmitting, accessing, collecting, monitoring, remotely storing users' Unique Device Identifiers ("UDIDs") involve a Trespass to Personal Property / Chattels?
- t) Is the Defendant liable under a theory of aiding and abetting one (1) more of the involved entities for violations of the statutes listed herein?
- u) Is the Defendant liable under a theory of civil conspiracy for violations of the statutes listed herein?
- v) Is the Defendant liable under a theory of unjust enrichment for violations of the statutes listed herein?
- w) Whether Defendant participated in and/or committed or is responsible for violation of law(s) complained of herein?
- x) Are Class Members entitled to damages as a result of the implementation of Defendant's marketing scheme, and, if so, what is the measure of those damages?
- y) Whether Plaintiffs and members of the Class have sustained damages as a result of Defendant's conduct, and, if so, what is the appropriate measure of damages?
- z) Whether Plaintiffs and members of the Class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and
- aa) Whether Plaintiffs and members of the Class are entitled to punitive damages, and, if so, in what amount?

278. **Typicality:** Plaintiffs' claims are typical of the claims of all of the other members of the Class, because his claims are based on the same legal and remedial theories as the claims of the Class and arise from the same course of conduct by Defendant.

279. **Adequacy of Representation:** Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel highly experienced in complex consumer Class action litigation, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

280. **Superiority:** A Class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members is relatively small compared to the burden and expense that would

1 be entailed by individual litigation of their claims against the Defendant. It would thus be  
 2 virtually impossible for the Class, on an individual basis, to obtain effective redress for the  
 3 wrongs done to them. Furthermore, even if Class Members could afford such individualized  
 4 litigation, the court system could not. Individualized litigation would create the danger of  
 5 inconsistent or contradictory judgments arising from the same set of facts. Individualized  
 6 litigation would also increase the delay and expense to all parties and the court system from the  
 7 issues raised by this action. By contrast, the Class action device provides the benefits of  
 8 adjudication of these issues in a single proceeding, economies of scale, and comprehensive  
 9 supervision by a single court, and presents no unusual management difficulties under the  
 10 circumstances here.

12 281. In the alternative, the Class may be also certified because:

- 13 a) the prosecution of separate actions by individual Class Members would create  
 14 a risk of inconsistent or varying adjudication with respect to individual Class  
 15 Members that would establish incompatible standards of conduct for the  
 Defendant;
- 16 b) the prosecution of separate actions by individual Class Members would create  
 17 a risk of adjudications with respect to them that would, as a practical matter,  
 18 be dispositive of the interests of other Class Members not parties to the  
 adjudications, or substantially impair or impede their ability to protect their  
 19 interests; and/or
- 20 c) Defendant have acted or refused to act on grounds generally applicable to the  
 Class thereby making appropriate final declaratory and/or injunctive relief  
 21 with respect to the members of the Class as a whole.

22 282. The claims asserted herein are applicable to all persons throughout the United  
 23 States that meet the class definition and class period.

24 283. The claims asserted herein are based on Federal law and California law, which is  
 25 applicable to all Class Members throughout the United States.

26 284. Adequate notice can be given to Class Members directly using information  
 27 maintained in Defendant's records or through notice by publication.  
 28

285. Damages may be calculated from the information maintained in Defendant's records, so that the cost of administering a recovery for the Class can be minimized. The amount of damages is known with precision from Defendant's records.

**First Cause of Action**  
**Violation of the Computer Fraud and Abuse Act**  
**18 U.S.C. § 1030 *et seq.***  
**Against Defendant OpenFeint**

286. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

287. Plaintiffs assert this claim against Defendant on behalf of themselves and the Class.

288. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as "CFAA," regulates fraud and relates activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

289. Defendant violated 18 U.S.C. § 1030 by intentionally accessing Plaintiffs' and Class Members' mobile computing device, without authorization by exceeding access, thereby obtaining information from such a protected device, causing the transmission to users' mobile devices, either by native installation or upgrade, of code that caused users' mobile devices to maintain, synchronize, and retain detailed, unencrypted location history files.

290. At all relevant times, Defendant engaged in business practices of transmitting code from within the Plaintiffs' and Class Members' downloaded applications so as to access their mobile devices to obtain a UDID and mobile device data. Such acts were conducted without authorization and consent of the Plaintiffs and Class Members.

291. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g), provides a civil cause of action to "any person who suffers damage or loss by reason of a violation" of CFAA.

1           292. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(i), makes it  
2 unlawful to “knowingly cause[s] the transmission of a program, information, code, or command  
3 and as a result of such conduct, intentionally cause[s] damage without authorization, to a  
4 protected computer,” of a loss to one or more persons during any one-year period aggregating at  
5 least \$5,000 in value.

6           293. Plaintiffs’ and Class Members’ computers are a “protected computer...which is  
7 used in interstate commerce and/or communication” within the meaning of 18 U.S.C. §  
8 1030(e)(2)(B).  
9

10          294. Defendant violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing a  
11 Plaintiffs’ and Class Members’ mobile computing device, without authorization or by exceeding  
12 access, thereby obtaining information from such a protected mobile computing device.

13          295. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the  
14 transmission of a command embedded within their webpage’s, downloaded to Plaintiffs’ and  
15 Class Members’ mobile computing device, which are protected mobile computing devices as  
16 defined in 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs’ and  
17 Class Members’ viewing habits, Defendant intentionally caused damage without authorization to  
18 those Plaintiffs’ and Class Members’ mobile computing devices by impairing the integrity of the  
19 computer.  
20

21          296. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally accessing  
22 Plaintiffs’ and Class Members’ protected mobile computing devices without authorization, and  
23 as a result of such conduct, recklessly caused damage to Plaintiffs’ and Class Members’ mobile  
24 computing devices by impairing the integrity of data and/or system and/or information.  
25

26          297. Defendant violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally accessing  
27 Plaintiffs’ and Class Members’ protected mobile computing devices without authorization, and  
28

1 as a result of such conduct, caused damage and loss to Plaintiffs and Class Members.

2 298. Plaintiffs and Class Members have suffered damage by reason of these violations,  
3 as defined in 18 U.S.C. § 1030(e)(8), by the “impairment to the integrity or availability of data, a  
4 program, a system or information.”

5 299. Plaintiffs and Class Members have suffered loss by reason of these violations, as  
6 defined in 18 U.S.C. § 1030(e)(11), by the “reasonable cost ... including the cost of responding to  
7 an offense, conducting a damage assessment, and restoring the data, program, system, or  
8 information to its condition prior to the offense, and any revenue lost, cost incurred, or other  
9 consequential damages incurred because of interruption of service.”  
10

11 300. Plaintiffs and Class Members have suffered loss by reason of these violations,  
12 including, without limitation, violation of the right of privacy, disclosure of Personal Identifiable  
13 Information, Sensitive Identifying Information, and Personal Information, interception, and  
14 transactional information that otherwise is private, confidential, and not of public record.

15 301. Defendant OpenFeint is liable for the violations of the Computer Fraud and Abuse  
16 Act alleged herein.  
17

18 302. As a result of these takings, Defendant’s conduct has caused a loss to one or more  
19 persons during any one-year period aggregating at least \$5,000 in value in real economic  
20 damages.

21 303. Plaintiffs and Class Members have additionally suffered loss by reason of these  
22 violations, including, without limitation, violation of the right of privacy.  
23

24 304. Defendant’s unlawful access to Plaintiffs’ and Class Members’ computers and  
25 electronic communications has caused Plaintiffs and Class Members irreparable injury. Unless  
26 restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs’ and Class  
27 Members’ remedy at law is not adequate to compensate it for these inflicted and threatened  
28

injuries, entitling Plaintiffs and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

**Second Cause of Action**  
**Violations of the Electronic Communications Privacy Act**  
**18 U.S.C. § 2510**  
**Against Defendant OpenFeint**

305. Plaintiffs incorporate by reference all paragraphs previously alleged herein.

306. Plaintiffs assert this claim against Defendant on behalf of themselves and the Class.

307. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as “ECPA,” regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to “willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication,” within the meaning of 18 U.S.C. § 2511(1).

308. Defendant violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiffs’ and Class Members’ electronic communications, without knowledge, consent, or authorization.

309. At all relevant times, Defendant engaged in business practices of intercepting the Plaintiffs’ and Class Members’ electronic communications which included endeavoring to intercept the transmission of a UDID from within their mobile device. Once the Defendant obtained the UDID they used such to aggregate mobile device data of the Plaintiffs and Class Members as they used their mobile device, browsed the Internet, and activated downloaded applications.

310. The contents of data transmissions from and to Plaintiffs’ and Class Members’ personal computers constitute “electronic communications” within the meaning of 18 U.S.C. §2510.

1           311. Plaintiffs and Class Members are “person[s] whose ... electronic communication  
2 is intercepted ... or intentionally used in violation of this chapter” within the meaning of 18  
3 U.S.C. § 2520.

4           312. Defendant violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting,  
5 endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept  
6 Plaintiffs’ and Class Members’ electronic communications.

7           313. Defendant violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing, or  
8 endeavoring to disclose, to any other person the contents of Plaintiffs’ and Class Members’  
9 electronic communications, knowing or having reason to know that the information was obtained  
10 through the interception of Plaintiffs’ and Class Members’ electronic communications.

11           314. Defendant violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring  
12 to use, the contents of Plaintiffs’ and Class Members’ electronic communications, knowing or  
13 having reason to know that the information was obtained through the interception of Plaintiffs’  
14 and Class Members’ electronic communications.

15           315. Defendant’s intentional interception of these electronic communications without  
16 Plaintiffs’ or Class Members’ knowledge, consent, or authorization was undertaken without a  
17 facially valid court order or certification.

18           316. Defendant intentionally used such electronic communications, with knowledge, or  
19 having reason to know, that the electronic communications were obtained through interception,  
20 for an unlawful purpose.

21           317. Defendant unlawfully accessed and used, and voluntarily disclosed, the contents  
22 of the intercepted communications to enhance their profitability and revenue through advertising.  
23 This disclosure was not necessary for the operation of Defendant’s system or to protect  
24 Defendant’s rights or property.  
25  
26  
27  
28



320. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

**Third Cause of Action**  
**Violation of California’s Computer Crime Law**  
**Penal Code § 502 *et seq.***  
**Against Defendant OpenFeint**

92

1           323. The California Computer Crime Law, California Penal Code § 502, referred to as  
2 “CCCL” regulates “tampering, interference, damage, and unauthorized access to lawfully created  
3 computer data and computer systems.”

4           324. Defendant violated California Penal Code § 502 by knowingly accessing,  
5 copying, using, made use of, interfering, and/or altering, data belonging to Plaintiffs and Class  
6 Members: (1) in and from the State of California; (2) in the home states of the Plaintiffs; and (3)  
7 in the state in which the servers that provided the communication link between Plaintiffs and the  
8 applications they interacted with were located.

9  
10           325. At all relevant times, Defendant’s business practices of accessing the Plaintiffs’  
11 and Class Members’ mobile devices initially in order to obtain their UDID, then on a systematic  
12 and continuous basis, Defendant accessed the Plaintiffs’ and Class Members’ mobile devices in  
13 order to obtain mobile device data and to monitor and collect data related to their browsing  
14 habits.

15  
16           326. Pursuant to California Penal Code § 502(b)(1), “Access means to gain entry to,  
17 instruct, or communicate with the logical, arithmetical, or memory function resources of a  
18 computer, computer system, or computer network.”

19           327. Pursuant to California Penal Code § 502(b)(6), “Data means a representation of  
20 information, knowledge, facts, concepts, computer software, computer programs or instructions.  
21 Data may be in any form, in storage media, or as stored in the memory of the computer or in  
22 transit or presented on a display device.”

23  
24           328. Defendant violated California Penal Code § 502(c)(1) by knowingly accessing  
25 and without permission, altering, and making use of data from Plaintiffs’ and Class Members’  
26 mobile devices in order to devise and execute business practices to deceive Plaintiffs and Class  
27  
28

1 Members into surrendering private electronic communications and activities for Defendant'  
2 financial gain, and to wrongfully obtain valuable private data from Plaintiffs.

3 329. Defendant violated California Penal Code § 502(c)(2) by knowingly accessing  
4 and without permission, taking, or making use of data from Plaintiffs' and Class Members'  
5 mobile devices.

6 330. Defendant violated California Penal Code § 502(c)(3) by knowingly and without  
7 permission, using and causing to be used Plaintiffs' and Class Members' mobile computing  
8 devices' services.

9 331. Defendant violated California Penal Code section 502(c)(3) by knowingly and  
10 without permission using and causing to be used Plaintiffs' and Class Members' computer  
11 services.

12 332. Defendant violated California Penal Code section 502(c)(4) by knowingly  
13 accessing and, without permission, adding and/or altering the data from Plaintiffs' and Class  
14 Members' computers, that is, application code installed on such computers.

15 333. Defendant violated California Penal Code section 502(c)(5) by knowingly and  
16 without permission disrupting or causing the disruption of Plaintiffs' and Class Members'  
17 computer services or denying or causing the denial of computer services to Plaintiffs and the  
18 Class.

19 334. Defendant violated California Penal Code § 502(c)(6) by knowingly and without  
20 permission providing, or assisting in providing, a means of accessing Plaintiffs' computers,  
21 computer system, and/or computer network.

22 335. Defendant violated California Penal Code § 502(c)(7) by knowingly and without  
23 permission accessing, or causing to be accessed, Plaintiffs' computer, computer system, and/or  
24 computer network.



“Any person who, . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . .”

344. At all relevant times, Defendant’s business practices of accessing the mobile device data of the Plaintiffs and Class Members was without authorization and consent; including but not limited to obtaining any and all communications involving their UDID.

345. On information and belief, each Plaintiff, and each Class Member, during one or more of their interactions on the Internet during the Class Period, communicated with one or more web entities based in California, or with one or more entities whose servers were located in California.

346. Communications from the California web-based entities to Plaintiffs and Class Members were sent from California. Communications to the California web-based entities from Plaintiffs and Class Members were sent to California.

347. Plaintiffs and Class Members did not consent to any of the Defendant’s actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

348. Plaintiffs and Class Members did not consent to any of the Defendant’s actions in using the contents of their communications with such California-based entities.

349. Defendant is not a “ public utility engaged in the business of providing communications services and facilities . . .”

350. Defendant’s actions alleged herein were not undertaken: “for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public

1 utility.”

2 351. Defendant’s actions alleged herein were not undertaken in connection with: “the  
3 use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of  
4 a public utility.

5 352. Defendant’s actions alleged herein were not undertaken with respect to any  
6 telephonic communication system used for communication exclusively within a state, county,  
7 city and county, or city correctional facility.

8 353. Defendant directly participated in the interception, reading, and/or learning the  
9 contents of the communications between Plaintiffs, Class Members and California-based web  
10 entities.

11 354. Alternatively, and of equal violation of the California Invasion of Privacy Act,  
12 Defendant aided, agreed with, and/or conspired with involved entities to unlawfully do, or  
13 permit, or cause to be done all of the acts complained of herein.

14 355. Plaintiffs and Class Members have additionally suffered loss by reason of these  
15 violations, including, without limitation, violation of the right of privacy.

16 356. Unless restrained and enjoined, Defendant will continue to commit such acts.  
17 Pursuant to Section 637.2 of the California Penal Code, Plaintiffs and the Class have been  
18 injured by the violations of California Penal Code section 631. Wherefore, Plaintiffs, on behalf  
19 of themselves and on behalf of a similarly situated Class of consumers, seek damages and  
20 injunctive relief.  
21  
22  
23

24 **Fifth Cause of Action**  
25 **Violation of the Consumer Legal Remedies Act**  
26 **(“CLRA”) California Civil Code § 1750, *et seq.***  
27 **Against Defendant OpenFeint**

28 357. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

358. In violation of Civil Code section 1750, *et seq.* (the “CLRA”), Defendant engaged

1 and is engaging in unfair and deceptive acts and practices in the course of transactions with  
2 Plaintiffs, and such transactions are intended to and have resulted in the sales of services to  
3 consumers. Plaintiffs and the Class Members are “consumers” as that term is used in the CLRA  
4 because they sought or acquired Defendant’s goods or services for personal, family, or  
5 household purposes.

6 359. At all relevant times, Defendant’s business practices of selling OpenFeint  
7 applications, or allowing OpenFeint application’s use for free, were goods Plaintiffs and Class  
8 Members obtained for use. Defendant’s scheme to offer such goods misleads the nature and  
9 integrity of the application since Defendant intended to use such for mobile device tracking.  
10

11 360. Defendant’s representations that its services have characteristics, uses, and  
12 benefits that they do not have, in violation of Civil Code § 1770(a)(5).

13 361. This cause of action is brought pursuant to the California Consumers Legal  
14 Remedies Act, Cal. Civ. Code § 1750 *et seq.* (the “CLRA”). This cause of action does not seek  
15 monetary damages at this point, but is limited solely to injunctive relief. Plaintiffs and Class  
16 Members will amend this Class Action Complaint to seek damages in accordance with the  
17 CLRA after providing the Defendant with notice pursuant to California Civil Code § 1782.  
18

19 362. At this time, Plaintiffs and Class Members seek only injunctive relief under this  
20 cause of action. Pursuant to California Civil Code, Section 1782, Plaintiffs will notify Defendant  
21 in writing of the particular violations of Civil Code, Section 1770 and demand that Defendant  
22 rectify the problems associated with its behavior detailed above, which acts and practices are in  
23 violation of Civil Code § 1770.  
24

25 363. If Defendant fails to respond adequately to Plaintiffs’ and Class Members’ above-  
26 described demand within 30 days of Plaintiffs’ notice, pursuant to California Civil Code, Section  
27 1782(b), Plaintiffs will amend the complaint to request damages and other relief, as permitted by  
28

Civil Code, Section 1780.

**Sixth Cause of Action**  
**Violation of Unfair Competition California Business and Professions Code § 17200**  
**Against Defendant OpenFeint**

364. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

365. In violation of California Business and Professions Code § 17200 et seq., Defendant' conduct in this regard is ongoing and includes, but is not limited to, unfair, unlawful and fraudulent conduct.

366. Defendant misled consumers by continuously and falsely representing during the Class Period that they would not make Personally Identifiable Information available to third parties as alleged herein.

367. At all relevant times, Defendant's business practices of merging its mobile devices and Application Developer's applications and services to Plaintiffs and Class Members by way of, *inter alia*, commercial marketing and advertising, misrepresented and/or omitted the truth about the extent to which Defendant would obtain and share Plaintiffs' and Class Members' Sensitive and Personal Identifiable Information with third parties.

368. Defendant engaged in these unfair and fraudulent practices to increase their profits. Had Plaintiffs known that Defendant would share their Personally Identifiable Information with third parties; they would not have purchased or used the Defendant's services, which in turn, forced them to relinquish, for free, valuable Personal Information.

369. By engaging in the above-described acts and practices, Defendant committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and/or property—specifically, Personal Information.



1           **A. Unlawful Business Act and Practices**

2           370. Defendant's business acts and practices are unlawful, in part, because they violate  
3 California Business and Professions Code § 17500, et seq., which prohibits false advertising, in  
4 that they were untrue and misleading statements relating to Defendant's performance of services  
5 and with the intent to induce consumers to enter into obligations relating to such services, and  
6 regarding statements Defendant knew were false or by the exercise of reasonable care Defendant  
7 should have known to be untrue and misleading.  
8

9           371. Defendant's business acts and practices are also unlawful in that they violate the  
10 California Consumer Legal Remedies Act, California Civil Code, Sections 1647, et seq., 1750, et  
11 seq., and 3344, California Penal Code, section 502, and Title 18, United States Code, Section  
12 1030. Defendant is therefore in violation of the "unlawful" prong of the UCL.  
13

14           **B. Unfair Business Act and Practices**

15           372. Defendant's business acts and practices are unfair because they cause harm and  
16 injury-in-fact to Plaintiffs and Class Members, and for which Defendant has no justification  
17 other than to increase, beyond what Defendant would have otherwise realized, its profit in fees  
18 from advertisers and its information assets through the acquisition of consumers' Personal  
19 Information.  
20

21           373. Defendant's conduct lacks reasonable and legitimate justification in that  
22 Defendant benefited from such conduct and practices while Plaintiffs and the Class Members  
23 have been misled as to the nature and integrity of Defendant's services and have, in fact, suffered  
24 material disadvantage regarding their interests in the privacy and confidentiality of their Personal  
25 Information. Defendant's conduct offends public policy in California tethered to the Consumer  
26 Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing  
27 the need for consumers to obtain material information that enables them to safeguard their own  
28

1 privacy interests, including California Civil Code, Section 1798.80.

2 374. In addition, Defendant's modus operandi constitutes a sharp practice in that  
3 Defendant knew and should have known that consumers care about the status of Personal  
4 Information and privacy but are unlikely to be aware of and able to detect the means by which  
5 Defendant was conducting themselves in a manner adverse to their commitments and users'  
6 interests, through the undisclosed functions of mobile devices and apps and the related conduct  
7 of the Defendant. Defendant is therefore in violation of the unfairness prong of the Unfair  
8 Competition Law.  
9

10 375. Defendant's acts and practices were fraudulent within the meaning of the Unfair  
11 Competition Law because they were likely to mislead the members of the public to whom they  
12 were directed.

13 376. Defendant's practice of capturing, storing, and transferring through  
14 synchronization to other computers highly detailed and personal records of users' location  
15 histories of long duration, and storing such information in unencrypted form, was in violation of  
16 the unfairness prong of the Unfair Competition Law.  
17

18 377. Plaintiffs, on behalf of themselves and on behalf of each member of the Class,  
19 seek individual restitution, injunctive relief, and other relief allowed under the UCL as the Court  
20 deems just and proper.

21 **Seventh Cause of Action**  
22 **Breach of Contract**  
23 **Against Defendant OpenFeint**

24 378. Plaintiffs hereby incorporate by reference the allegations contained in all of the  
25 preceding paragraphs of this complaint.

26 379. Plaintiffs and Class Members entered into a contract with Defendant OpenFeint in  
27 order to use the OpenFeint Store apps. This contract had rights, obligations, and duties between  
28

1 Plaintiffs and Class Members and Defendant OpenFeint, including but not limited to, protecting  
2 the privacy of its users.

3 380. Plaintiffs and Class Members activities involved in their use of the OpenFeint  
4 App Store included, but was not limited to, providing Personal Identifiable Information to  
5 Defendant OpenFeint; furthermore Defendant OpenFeint designed the Plaintiffs' and Class  
6 Members' mobile device data, including but not limited to, their mobile devices' UDID with  
7 third parties, including Application Developers and Application Developers Affiliates, in  
8 violation of its own contract with Plaintiffs and Class Members.  
9

10 381. Plaintiffs and Class Members did not have notice, nor consent to, Defendant  
11 OpenFeint sharing their mobile devices UDID with Application Developers or Application  
12 Developers' Affiliates.

13 382. Plaintiffs and Class Members have performed their obligation pursuant to  
14 Defendant OpenFeint's contract.  
15

16 383. Defendant OpenFeint has materially breached its contractual obligations through  
17 its conduct.

18 384. Plaintiffs and Class Members have been damaged as a direct and proximate result  
19 of Defendant OpenFeint's breach of their contract.

20 **Eighth Claim For Relief**  
21 **Breach of Implied Covenant of Good Faith and Fair Dealing**  
22 **Against Defendant OpenFeint**

23 385. Plaintiffs hereby incorporate by reference the allegations contained in all of the  
24 preceding paragraphs in this complaint.

25 386. As set forth above, Plaintiffs and Class Members submit Personal Information to  
26 OpenFeint and such information is stored on Plaintiffs' and Class Members' mobile devices, and  
27 OpenFeint promises in its Privacy Policy that it will not share this information with third-party  
28

1 advertisers or Application Developers without Plaintiffs' consent, and the consent of each Class  
2 Member, respectively, and promises in its click-through agreement to protect users' privacy.

3 387. A covenant of good faith and fair dealing, which imposes upon each party to a  
4 contract a duty of good faith and fair dealing in its performance, is implied in every contract,  
5 including their agreement in the transactions for acquisitions of Defendant OpenFeint's  
6 applications that embodies the relationship between OpenFeint and its users.

7 388. Good faith and fair dealing is an element imposed by common law or statute as an  
8 element of every contract under the laws of every state. Under the covenant of good faith and fair  
9 dealing, both parties to a contract impliedly promise not to violate the spirit of the bargain and  
10 not to intentionally do anything to injure the other party's right to receive the benefits of the  
11 contract.  
12

13 389. Plaintiffs and Class Members reasonably relied upon OpenFeint to act in good  
14 faith with regard to the contract and in the methods and manner in which it carries out the  
15 contract terms. Bad faith can violate the spirit of their agreements and may be overt or may  
16 consist of inaction. OpenFeint's inaction in failing to adequately notify Plaintiffs and Class  
17 Members of the release of their Personal Information to the Application Developers, and by  
18 Application Developers Affiliates, depriving Plaintiffs and Class Members of the means to  
19 discover their information was "leaked," thus evidencing bad faith and ill motive.  
20

21 390. The contract is a form contract, the terms of which Plaintiffs are deemed to have  
22 accepted once Plaintiffs and the Class signed up with OpenFeint. The contract purports to give  
23 discretion to OpenFeint relating to its protection of users' privacy. OpenFeint is subject to an  
24 obligation to exercise that discretion in good faith. The covenant of good faith and fair dealing is  
25 breached when a party to a contract uses discretion conferred by the contract to act dishonestly or  
26 to act outside of accepted commercial practices. OpenFeint breached its implied covenant of  
27  
28

1 good faith and fair dealing by exercising bad faith in using its discretionary rights to deliberately,  
2 routinely, and systematically make Plaintiffs' and Class Members' personal information  
3 available to third parties.

4 391. Plaintiffs and Class Members' have performed all, or substantially all, of the of  
5 the obligations imposed on them under contract, whereas OpenFeint has acted in a manner as to  
6 evade the spirit of the contract, in particular by deliberately, routinely, and systematically  
7 without notifying Plaintiffs and Class Members of its disclosure of Plaintiffs' and Class  
8 Members' personal information to Affiliates, and by Developers. Such actions represent a  
9 fundamental wrong that is clearly beyond the reasonable expectation of the parties. OpenFeint's  
10 causing the disclosure of such information to the Affiliates, and by Developers is not in  
11 accordance with the reasonable expectations of the parties and evidences a dishonest motive.

12 392. OpenFeint's ill motive is further evidenced by its failure to obtain Plaintiffs' and  
13 Class Members' consent in data mining efforts while at the same time consciously and  
14 deliberately facilitating data mining to automatically and without notice provide user information  
15 the Affiliates, and by Developers. OpenFeint profits from advertising revenues derived from its  
16 data mining efforts from Plaintiffs and the Class.

17 393. The obligation imposed by the implied covenant of good faith and fair dealing is  
18 an obligation to refrain from opportunistic behavior. OpenFeint has breached the implied  
19 covenant of good faith and fair dealing in their agreement through its policies and practices as  
20 alleged herein. Plaintiffs and the Class have sustained damages and seek a determination that the  
21 policies and procedures of OpenFeint are not consonant with OpenFeint's implied duties of good  
22 faith and fair dealing.

23 394. OpenFeint's capture, retention, and transfer through synchronization of users'  
24 detailed location histories, even when such users had disabled GPS services on their mobile  
25

1 devices, and storing such location histories in unencrypted form, was a breach of the implied  
2 covenant of good faith and fair dealing.

3 **Ninth Cause of Action**  
4 **Conversion**  
5 **Against Defendant OpenFeint**

6 395. Plaintiffs hereby incorporate by reference the allegations contained in all of the  
7 preceding paragraphs of this complaint.

8 396. Plaintiffs' and Class Members' mobile device data, including but not limited to  
9 their mobile devices' UDID is being used by Defendant to obtain sensitive and Personal  
10 Identifiable Information derived from Plaintiffs' and Class Members' mobile browsing activities.  
11 Such property, owned by the Plaintiffs and Class Members, is valuable to the Plaintiffs and Class  
12 Members.

13 397. Plaintiffs' and Class Members' mobile devices use bandwidth. Defendant's  
14 activities, made the basis of this action, used without notice or authorization, such bandwidth for  
15 purposes not contemplated, not agreed to, by Plaintiffs and Class Members when they  
16 downloaded Application Developer's applications. Such property, owned by the Plaintiffs and  
17 Class Members, is valuable to the Plaintiffs and Class Members.

18 398. Defendant unlawfully exercised dominion over said property and thereby  
19 converted Plaintiffs' and Class Members' property, by providing Sensitive and Personally  
20 Identifying Information to third parties and by using Plaintiffs' and Class Members' bandwidth  
21 for data mining, in violation of the collective allegations, made the basis of this action.

22 399. Plaintiffs and Class Members were damaged thereby.  
23  
24  
25  
26  
27  
28

**Tenth Cause of Action  
Negligence  
Against Defendant OpenFeint**

400. Plaintiffs incorporate the above allegations by reference as if fully set forth herein.

401. As set forth above, OpenFeint owed a duty to Plaintiffs and Class Members.

402. OpenFeint breached its duty by designing a mobile platform so that the Application Affiliates and Application Developers could acquire Personal Information without consumers' knowledge or permission, by failing to review and remove privacy-violating apps from the OpenFeint Application Market, and by constructing and controlling consumers' user experience and mobile environment so that consumers could not reasonably avoid such privacy-affecting actions.

403. OpenFeint failed to fulfill its own commitments and, further, failed to fulfill even the minimum duty of care to protect Plaintiffs' and Class Members' Personal Information, privacy rights, and security.

404. OpenFeint's failure to fulfill its commitments included its practice of capturing frequent and detailed information about users' "Fine" locations for unreasonable retention periods, maintaining records of such location histories on users, transferring such location history files to users' replacement mobile device, transferring such location history files to other mobile devices with which users synchronized their mobile devices, and storing such location history files in accessible, unencrypted form, all without providing notice to users or obtaining users' consent, and where consumers had no reasonable means to become aware of such practice or to manage it, and where such practice placed users at unreasonable risk of capture and misuse of such highly detailed and Personal Information, and where a reasonable consumer would consider such a practice unexpected, objectionable, and shocking to the conscience of a reasonable person.

1           405.   OpenFeint's unencrypted cloud storage which was synchronized the information  
2 described above was negligent.

3           406.   Plaintiffs and Class Members were harmed as a result of OpenFeint's breach of its  
4 duties, and OpenFeint proximately caused such harms.

5                                   **Eleventh Cause of Action**  
6                                   **Trespass to Personal Property / Chattels**  
7                                   **Against Defendant OpenFeint**

8           407.   Plaintiffs incorporate by reference all paragraphs previously alleged herein.

9           408.   The common law prohibits the intentional intermeddling with personal property,  
10 including a mobile device, in possession of another which results in the deprivation of the use of  
11 the personal property or impairment of the condition, quality, or usefulness of the personal  
12 property.

13           409.   By engaging in the acts alleged in this complaint without the authorization or  
14 consent of Plaintiffs and Class Members, Defendant dispossessed Plaintiffs and Class Members  
15 from use and/or access to their mobile devices, or parts of them. Further, these acts impaired the  
16 use, value, and quality of Plaintiffs' and Class Members' mobile device. Defendant's acts  
17 constituted an intentional interference with the use and enjoyment of their mobile devices. By the  
18 acts described above, Defendant has repeatedly and persistently engaged in trespass to personal  
19 property in violation of the common law.

20           410.   Without Plaintiffs' and Class Members' consent, or in excess of any consent  
21 given, Defendant knowingly and intentionally accessed Plaintiffs' and Class Members' property,  
22 thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property  
23 and causing injury to Plaintiffs and the members of the Class.

24           411.   Defendant engaged in deception and concealment in order to gain access to  
25 Plaintiffs' and Class Members' mobile devices.

26           412.   Defendant undertook the following actions with respect to Plaintiffs' and Class  
27  
28



Members' mobile devices:

- a) Defendant accessed and obtained control over the users' mobile device;
- b) Defendant caused the installation of code on the hard drives of the mobile devices;
- c) Defendant programmed the operation of its code to circumvent the mobile device owners privacy and security controls, to remain beyond their control, and to continue function and operate without notice to them or consent from Plaintiffs and Class Members;
- d) Defendant obtained users' UDID from a tracking code on the users' mobile device; and
- e) Defendant used the users' UDID to obtain without notice or consent, mobile browsing activities of the mobile device, and outside of the control of the owner of the mobile device.

413. All these acts described above were acts in excess of any authority any user granted when he or she visited the Defendant OpenFeint's Application Market and downloaded one (1) or more of the Defendant OpenFeint affiliated applications and none of these acts was in furtherance of users viewing the applications. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and Class Members may have granted to Defendant OpenFeint and/or Application Developers was invalid.

414. Defendant's installation and operation of its program used, interfered, and/or intermeddled with Plaintiffs' and Class Members' mobile devices. Such use, interference and/or intermeddling was without Plaintiffs' and Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class Members' consent.

415. Defendant's installation and operation of its program constitutes trespass, nuisance, and an interference with Plaintiffs' and Class Members' chattels, to wit, their mobile

1 devices.

2 416. Defendant's installation and operation of its program impaired the condition and  
3 value of Plaintiffs' and Class Members' mobile devices.

4 417. Defendant's trespass to chattels, nuisance, and interference caused real and  
5 substantial damage to Plaintiffs and Class Members.

6 418. As a direct and proximate result of Defendant's trespass to chattels, nuisance,  
7 interference, unauthorized access of and intermeddling with Plaintiffs' and Class Members'  
8 property, Defendant injured and impaired in the condition and value of Class Members' mobile  
9 devices, as follows:  
10

- 11 a) By consuming the resources of and/or degrading the performance of  
12 Plaintiffs' and Class Members' mobile devices (including space, memory,  
13 processing cycles, Internet connectivity, and unauthorized use of their  
bandwidth);
- 14 b) By diminishing the use of, value, speed, capacity, and/or capabilities of  
15 Plaintiffs' and Class Members' mobile devices;
- 16 c) By devaluing, interfering with, and/or diminishing Plaintiffs' and Class  
17 Members' possessory interest in their mobile devices;
- 18 d) By altering and controlling the functioning of Plaintiffs' and Class Members'  
19 mobile devices;
- 20 e) By infringing on Plaintiffs' and Class Members' right to exclude others from  
21 their mobile devices;
- 22 f) By infringing on Plaintiffs' and Class Members' right to determine, as owners  
23 of/or their mobile devices, which programs should be installed and operating  
24 on their mobile devices;
- 25 g) By compromising the integrity, security, and ownership of Plaintiffs' and  
26 Class Members' mobile devices; and
- 27 h) By forcing Plaintiffs and Class Members to expend money, time, and  
28 resources in order to remove the program installed on their mobile devices  
without notice or consent.

**PRAYER FOR RELIEF**

1 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, prays  
 2 for judgment against Defendant as follows:

3 A. Certify this case as a Class action on behalf of the Classes defined above, appoint  
 4 Plaintiffs as Class representatives, and appoint their counsel as Class counsel;  
 5

6 B. Declare that the actions of Defendant, as set out above, violate the following:

7 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

8 b) Electronic Communications Privacy Act 18 U.S.C. § 2510;

9 c) California's Computer Crime Law, Penal Code § 502;

10 d) California Invasion of Privacy Act, Penal Code § 630;

11 e) Consumer Legal Remedies Act, ("CLRA") California Civil Code § 1750;

12 f) Unfair Competition, California Business and Professions Code § 17200;

13 g) Breach of Contract;

14 h) Breach of Implied Covenant of Good Faith and Fair Dealing;

15 i) Conversion;

16 j) Negligence;

17 k) Trespass to Personal Property / Chattels; and  
 18

19 C. As applicable to the Classes *mutatis mutandis*, awarding injunctive and equitable relief  
 20 including, *inter alia*: (i) prohibiting Defendant from engaging in the acts alleged above;  
 21 (ii) requiring Defendant to disgorge all of its ill-gotten gains to Plaintiffs and the other  
 22 Class Members, or to whomever the Court deems appropriate; (iii) requiring Defendant  
 23 to delete all data surreptitiously or otherwise collected through the acts alleged above;  
 24 (iv) requiring Defendant to provide Plaintiffs and the other Class Members a means to  
 25 easily and permanently decline any participation in any data collection activities; (v)  
 26 awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired  
 27 by Defendant by means of the wrongful conduct alleged herein; and (vi) ordering an  
 28 accounting and constructive trust imposed on the data, funds, or other assets obtained by  
 unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or  
 concealment of such assets by Defendant;

D. Award damages, including statutory damages where applicable, to Plaintiffs and Class  
 Members in an amount to be determined at trial;

1 E. Award restitution against Defendant for all money to which Plaintiffs and the Classes are  
entitled in equity;

2 F. Restrain Defendant, its officers, agents, servants, employees, and attorneys, and those in  
3 active concert or participation with them from continued access, collection, and  
4 transmission of Plaintiffs' and Class Members' Personal Information via preliminary and  
permanent injunction;

5 G. Award Plaintiffs and the Classes:

6 a) their reasonable litigation expenses and attorneys' fees;

7 b) pre- and post-judgment interest, to the extent allowable;

8 c) restitution, disgorgement and/or other equitable relief as the Court deems  
9 proper;

10 d) compensatory damages sustained by Plaintiffs and all others similarly situated  
11 as a result of Defendant's unlawful acts and conduct;

12 e) statutory damages, including punitive damages; and

13 f) permanent injunction prohibiting Defendant from engaging in the conduct and  
14 practices complained of herein.

15 H. For such other and further relief as this Court may deem just and proper.

16 Dated this 22<sup>nd</sup> day of June 2011



By: David C. Parisi

18 David C. Parisi (SBN 162248)  
19 dparisi@parisihavens.com  
20 PARISI & HAVENS LLP  
21 15233 Valleyheart Drive  
22 Sherman Oaks, CA 91403  
Telephone: (818) 990-1299  
Fax: (818) 501-7852

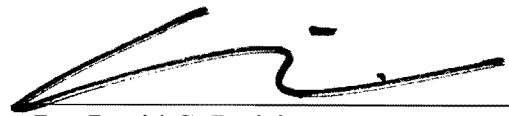
23 Joseph H. Malley (not yet admitted)  
24 malleylaw@gmail.com  
25 LAW OFFICE OF JOSEPH H. MALLEY, P.C.  
26 1045 North Zang Blvd  
27 Dallas, TX 75208  
28 Telephone: (214) 943-6100  
Fax: (214) 943-6170

*Counsel for Plaintiffs*

**JURY TRIAL DEMAND**

The Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated this 22<sup>nd</sup> day of June 2011



By: David C. Parisi

David C. Parisi (SBN 162248)

dparisi@parisihavens.com

PARISI & HAVENS LLP

15233 Valleyheart Drive

Sherman Oaks, CA 91403

Telephone: (818) 990-1299

Fax: (818) 501-7852

Joseph H. Malley (not yet admitted)

malleylaw@gmail.com

LAW OFFICE OF JOSEPH H. MALLEY, P.C.

1045 North Zang Blvd

Dallas, TX 75208

Telephone: (214) 943-6100

Fax: (214) 943-6170

*Counsel for Plaintiffs*

**DECLARATION OF DAVID C. PARISI**

I, David C. Parisi, hereby declare on oath as follows:

1. I am an attorney licensed to practice law in the state of California. I am over the age of 18 years and I have personal knowledge of the matters attested to herein. If called upon to testify, I would and could competently do so.

2. I make this declaration pursuant to California Civil Code section 1780(c) on behalf of my clients, plaintiffs Matthew Hines, Jennifer Aguirre and Alexander Hernandez.

3. Defendant Openfeint, Inc.'s principle executive offices and headquarters are located at 1999 S. Bascom Ave., Suite 925, Campbell, California 95008.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Dated this 22<sup>nd</sup> day of June, 2011 at Sherman Oaks, California.



David C. Parisi